Bekijk de inventarisatie

DNSSEC-beveiliging Nederlandse domeinnamen onder de maat

DNSSEC-inventarisatie | februari 2017

SIDN Jouw wereld. Ons domein.

Inhoud

1 Managementsamenvatting

- Op dit moment is 46% van de .nl-domeinen ondertekend. Dat aandeel groeit nog steeds, al is de initiële snelle groei inmiddels wel afgevlakt. Daarmee hebben de voorlichting, trainingen, begeleiding bij implementatie, lobby, stimuleren van 'portfolio signing' en de incentive regeling van SIDN hun werk gedaan.

- Inmiddels zien we de opkomst van nieuwe veiligheidstoepassingen die boven op de cryptografisch beveiligde infrastructuur van DNSSEC geïmplementeerd worden:
  - DKIM, SPF en DMARC om phishing en spoofing tegen te gaan,
  - DANE voor de hoognodige extra beveiliging van TLS-certificaten voor web en mail.

- Daarmee is DNSSEC van een technologie-gedreven kostenpost overgegaan in een enabler voor belangrijke beveiligingstoepassingen.

- Hoewel de globale stijging van het aandeel DNSSEC-ondertekende domeinnamen duidelijk is terug te zien in vrijwel alle gemeten categorieën, zijn er nog steeds grote verschillen.

- Overheden zitten inmiddels met een aandeel van 59% ondertekende domeinnamen in de top van de ranglijst. Dat is met name te danken aan de opname van DNSSEC in de 'pas toe of leg uit'-lijst (ptolu) van het Forum Standaardisatie en de lancering van de Internet.nl portal.

- Ondanks dat wij van mening zijn dat de banken de belangrijkste gebruikers van DNSSEC zouden moeten zijn, scoren zij het slechtst van allemaal. Net als twee-en-half jaar geleden heeft slechts een enkeling zijn domeinnaam ondertekend. Met het opdoeken van de bankkantoren en het verminderen van het aantal pinautomaten is de online voordeur van de banken steeds belangrijker geworden. Bovendien hebben zij het meest van alle online bedrijven last van phishing, iets waar onder andere DNSSEC in combinatie met DKIM bescherming tegen kan bieden.

- Ook de mobiele telecom-aanbieders, access providers, service providers en de ondernemingen verantwoordelijk voor de datatransport-backbone doen het opvallend slecht. Slechts een klein deel van deze bedrijven heeft zijn domeinnaam ondertekend. Hetzelfde geldt voor de validerende zijde; de twee grootste Nederlandse access providers (KPN en Ziggo) doen geen validatie voor hun klanten. Deze bevindingen staan dan ook in schril contrast met de positionering van de Nederlandse digitale infrastructuur als de derde mainport naast Schiphol en de Rotterdamse haven.

2 Inleiding

DNSSEC

DNSSEC is een cryptografisch beveiligingssysteem voor DNS, de internet-adresgids die zorgt voor de vertaling van domeinnamen naar IP-adressen (en andersom). DNSSEC voorziet de DNS-informatie (de records) van een digitale handtekening, zodat de client (d.w.z. de resolver) kan controleren of de inhoud authentiek is.

DNSSEC is een voorwaarts compatibele uitbreiding van het DNS-protocol. Dat betekent dat resolvers en name servers zonder problemen met elkaar kunnen samenwerken, ongeacht of zij DNSSEC ondersteunen. Het beveiligingssysteem is echter alleen in werking als beide zijden DNSSEC ondersteunen. Daarvoor moet de betreffende domeinnaam ondertekend zijn (aan server-zijde) en moeten de digitale handtekeningen inderdaad geverifieerd worden (aan client-zijde). Alleen dan is de integriteit van de name server en het transport van de DNS-informatie beschermd.

Belang

Voor bedrijven is veel van de interactie met klanten, partners en leveranciers al naar internet verschoven. Ook overheden en andere organisaties communiceren onderling en met burgers en bedrijven steeds meer via internet. Daarmee is ook het belang van een goed beveiligde digitale ingang sterk toegenomen. Bezoekers moeten ook online op de betrouwbaarheid van een merk of organisatie kunnen rekenen. Een onveilige internet-dienst – laat staan een kraak – levert zowel reputatie- als zakelijke/financiële schade op.

Weet een kwaadwillende de DNS-informatie op de name-server, onderweg of bij de client te veranderen, dan kan hij die client naar een valse server sturen. Op die manier kunnen paswoorden en andere vertrouwelijke gegevens worden buitgemaakt, of geld en omzet worden gestolen.

DNSSEC beschermt de integriteit van de name server en het transport van de DNS-informatie. Dat is voor aanbieders van internet-diensten een garantie dat verkeer van bezoekers inderdaad op de juiste plaats terecht komt.

Historie

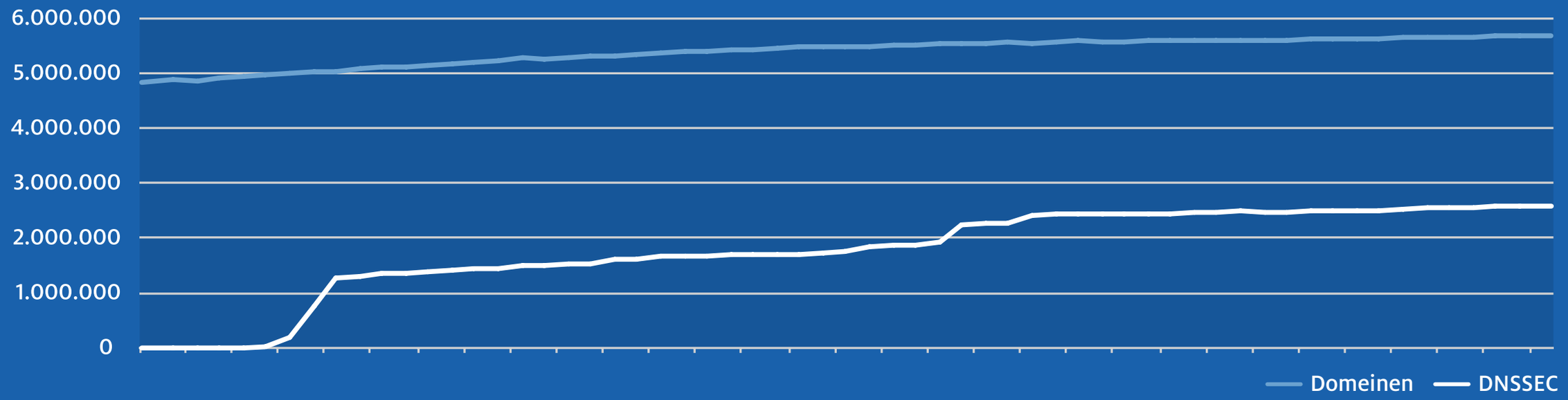
De afgelopen jaren heeft SIDN groot ingezet op DNSSEC, de crypto-grafische beveiliging van domeinnaam-informatie. Dat begon in 2010 met de ondertekening van ons eigen .nl top-level domein en het Friends & Family programma waarmee de eerste houders hun domein van een digitale handtekening konden voorzien. De grote doorbraak kwam twee jaar later met de incentive-regeling die de registrars een korting geeft op ondertekende domeinnamen.

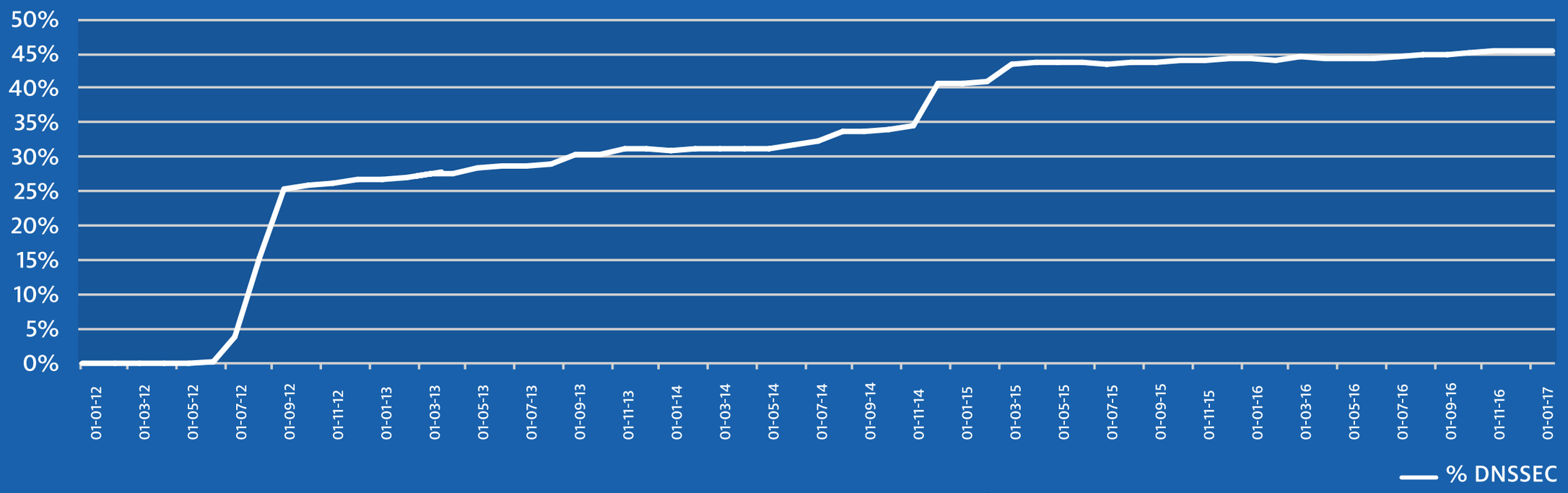
Stand van zaken *)

Inmiddels zijn 2.595.754 van de 5.701.008 nl-domeinen ondertekend (46%). Dat aandeel neemt nog steeds toe, al is die hele snelle groei inmiddels wel afgevlakt. De afgelopen twee jaar hebben we geen grote DNSSEC-projecten meer gezien van registrars die hun domeinnamen met honderdduizenden tegelijk ondertekenden. Alle registrars met een dergelijk groot portfolio aan .nl-domeinen hebben DNSSEC inmiddels ingevoerd, waarmee de integrale aanpak van SIDN met de incentive-regeling wat dat betreft zijn werk heeft gedaan.

› Figuur 1: DNSSEC-ondertekende .nl-domeinnamen, (absoluut) vanaf 2012
› Figuur 2: DNSSEC-ondertekende .nl-domeinnamen, (relatief) vanaf 2012

*) *op 8 februari 2017*





Figuur 1: DNSSEC-ondertekende .nl-domeinnamen (absoluut), vanaf 2012
Figuur 2: DNSSEC-ondertekende .nl-domeinnamen (relatief), vanaf 2012 [bron: SIDN]

2 Inleiding

De afgelopen twee jaar hebben we wel steeds vaker kunnen berichten over het gebruik van nieuwe veiligheidstoepassingen die bovenop de crypografisch beveiligde infrastructuur van DNSSEC geïmplementeerd worden: het drietal DKIM, SPF en DMARC om phishing, spamming, spoofing en andere e-mail-malware tegen te gaan, en DANE voor de broodnodige extra beveiliging van de TLS-certificaten voor web ('het sleuteltje') en mail.
> Figuur 3: .nl-domeinnamen die DANE gebruiken

DNSSEC en DKIM stonden al langer op de 'pas toe of leg uit'-lijst (ptolu) van het Forum Standaardisatie. Dat betekent dat overheidsorganisaties bij de vernieuwing van hun systemen min-of-meer verplicht zijn om deze standaarden te implementeren. Onlangs zijn STARTTLS en DKIM voor mail daar bij gekomen. De lancering van de Internet.nl portal, waar domeinnamen gecontroleerd kunnen worden op het gebruik van moderne en veilige internet-standaarden, is onderdeel van deze ontwikkeling.

Met de implementatie en het gebruik van nieuwe toepassings-mogelijkheden boven op de DNSSEC-infrastructuur is ook de positie van DNSSEC in belangrijke zin veranderd: deze beveiligingsstandaard is hiermee van technologie-gedreven kostenpost overgegaan in een enabler voor belangrijke beveiligingstoepassingen.

Validatie

De waarde van DNSSEC zit uiteindelijk in de validatie van de ondertekende domeinnamen door bezoekers en gebruikers daarvan. Daarmee zijn validatie en ondertekening complementair aan elkaar, en beide nodig om deze cryptografisch beveiligde infrastructuur te kunnen uitnutten (in de DNSSEC-wereld wel bekend als 'het kip-ei probleem').

> Figuur 4: DNSSEC queries (relatief)
> Figuur 5: DNSSEC queries (absoluut)

Een ouder argument voor organisaties die zelf hun DNS beheren was dat maar een beperkt aantal Internet-providers validatie deed voor zijn gebruikers. Hoewel het nog wachten is op de twee grootste (KPN en Ziggo), zijn er inmiddels flink wat Internet-providers (waaronder XS4All, BIT en Edutel) die wel valideren voor hun klanten. Een deel daarvan heeft de ondersteuning van DNSSEC ook expliciet naar hun klanten gecommuniceerd, waarmee de implementatie van DNSSEC ook commerciële waarde heeft gekregen.
> Figuur 6: DNSSEC queries van resolvers op Nederlandse netwerken
> Figuur 7: DNSSEC queries van resolvers op Nederlandse netwerken, in de tijd

Hoewel SIDN zelf in principe geen directe relatie heeft met de Internet-providers (voor zo ver zij niet ook registrar zijn), probeert zij toch ook de validatie van DNSSEC te stimuleren. Voorbeelden daarvan zijn de participatie in het Internet.nl portal-project en de lancering onlangs van de Valibox, een apparaatje waarmee eindgebruikers hun draadloze thuis/kantoor-netwerk van DNSSEC-validatie kunnen voorzien.

Een grote sta-in-de-weg voor validatie, een relatief groot aantal bogus domeinnamen in de .nl zone, behoort inmiddels tot de verleden tijd.
> Figuur 8: Totaal aantal gevonden validatiefouten over 2016.
> Figuur 9: Aantal registrars met gevonden validatiefouten, over 2016

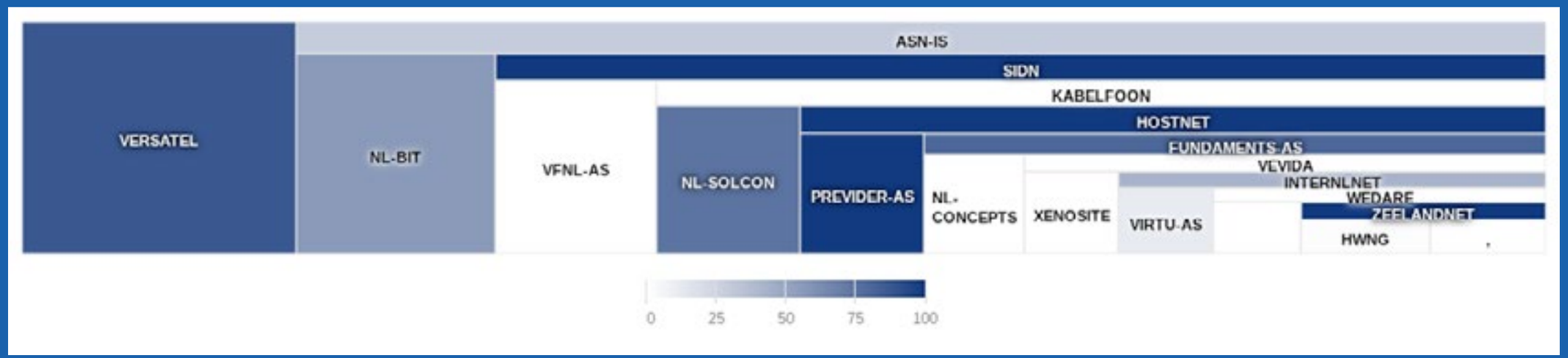
.nl-domeinnamen die DANE gebruiken

Figuur 3: .nl-domeinnamen die DANE gebruiken [8 februari 2017; bron: http://stats.sidnlabs.nl/#/dnssec/#dane]

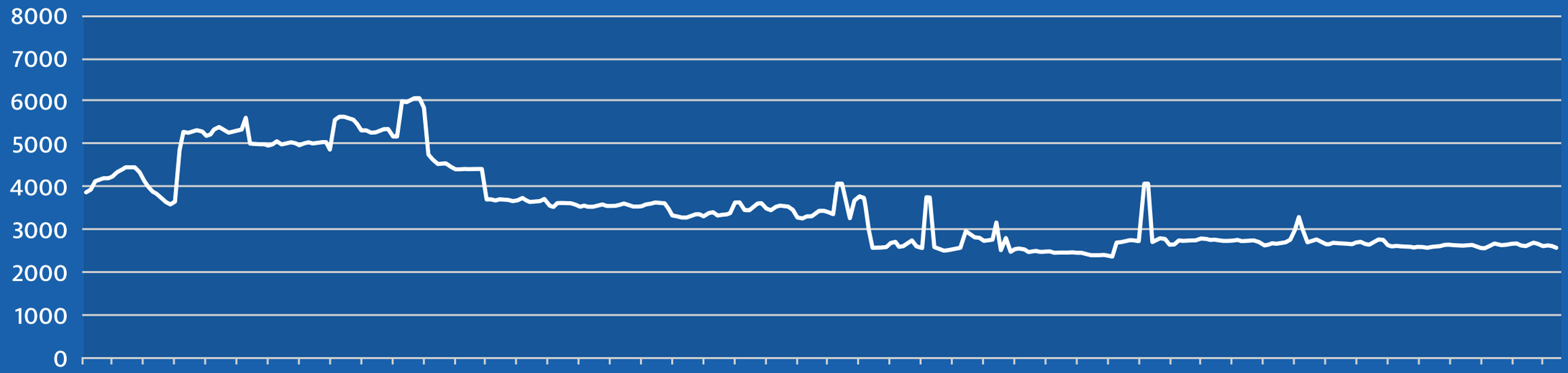
DNSSEC queries 1

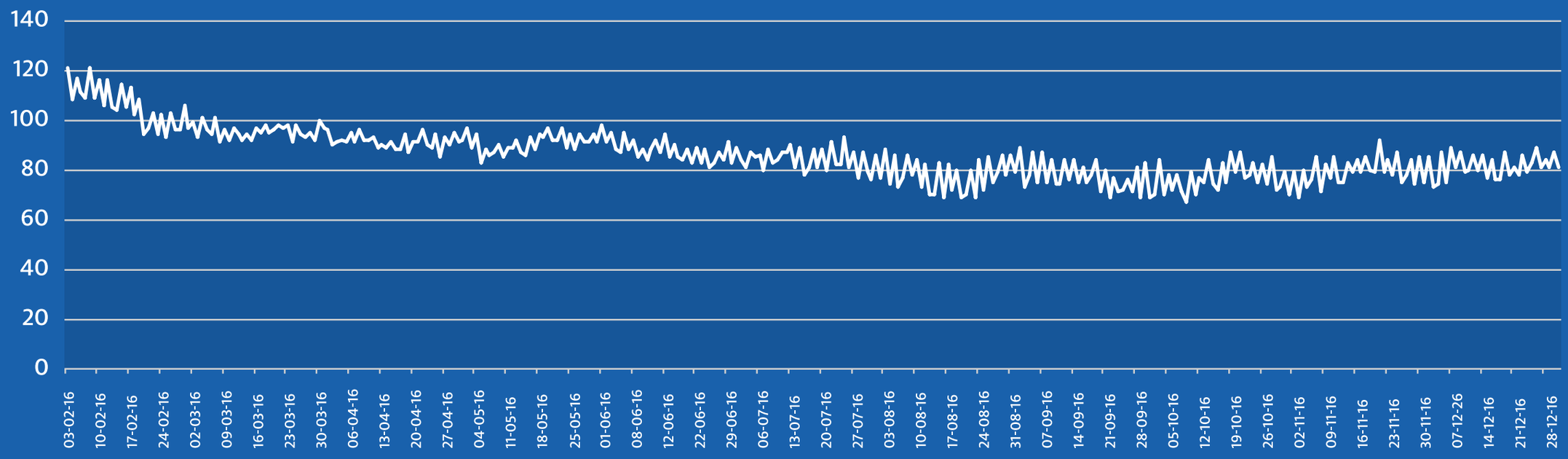
Figuur 4: DNSSEC queries (relatief) [8 februari 2017; bron: http://stats.sidnlabs.nl/#/dnssec/#query]
Figuur 5: DNSSEC queries (absoluut) [8 februari 2017; bron: http://stats.sidnlabs.nl/#/dnssec/#resolver]

DNSSEC queries 2



Figuur 6: DNSSEC queries van resolvers op Nederlandse netwerken [8 februari 2017; bron: http://stats.sidnlabs.nl/#/dnssec/#sharenl]
Figuur 7: DNSSEC queries van resolvers op Nederlandse netwerken, in de tijd [8 februari 2017; bron: http://stats.sidnlabs.nl/#/dnssec/#sharenlts]





Figuur 8: Totaal aantal gevonden validatiefouten, over 2016 [bron: SIDN]
Figuur 9: Aantal registrars met gevonden validatiefouten, over 2016 [bron: SIDN]

3 DNSSEC-inventarisatie 2017

Om beter inzicht te krijgen in de opbouw van het beveiligde domeinbestand hebben we gedetailleerder gekeken naar de toepassing van DNSSEC in verschillende sectoren. Wat je zou hopen en verwachten is dat organisaties waar veiligheid, geloofwaardigheid en betrouwbaarheid een belangrijke rol spelen hun hoofddomeinen vaker dan gemiddeld ondertekend hebben.

Voor deze inventarisatie zijn 27 lijstjes met domeinnamen gemaakt – deels met de hand verzameld, deels overgenomen van brancheorganisaties. Dat is een flinke uitbreiding ten opzichte van de eerste inventarisatie, uitgevoerd in het najaar van 2014.

Bij de selectie van de verschillende categorieën hebben we specifiek gekeken naar segmenten waarvan we menen dat de beveiliging met DNSSEC belangrijker is dan voor andere. Denk aan banken, internetwinkels, grote ondernemingen, overheidsorganisaties en kranten. Maar ook van internet- en telecom-providers verwachtten we meer. Zij hebben immers meer netwerk- en security-gerelateerde expertise in huis en kunnen DNSSEC zelf als dienst aan hun klanten aanbieden.

Voor de afzonderlijke categorieën is vervolgens onderzocht hoe groot het aandeel ondertekende domeinnamen is. Daarvoor is gebruik gemaakt van de DNSSEC Portfolio Checker van SIDN Labs.

4 Uitkomsten

De tabel hierna geeft een overzicht van onze bevindingen, gegroepeerd in een viertal sectoren. De kolommen met de categorieën en de percentages ondertekende domeinnamen zijn het meest interessant. Doorklikken op de categorie geeft een gedetailleerd overzicht van de onderzochte domeinen en de uitkomsten van onze meting.

Zoals de tabel laat zien, meten we nog steeds grote verschillen tussen de afzonderlijke categorieën. Tegelijkertijd zien we de stijging van het aandeel DNSSEC-ondertekende domeinnamen in de gehele .nl-zone ook duidelijk terug in een stijging over de afzonderlijke categorieën (waar voor een klein gedeelte ook andere dan .nl-domeinen bij zitten).

Waar twee-en-half jaar geleden met name de financiële dienstverleners, grote ondernemingen, overheden en internet-providers nog een grote achterstand ten opzichte van de rest hadden, is dat inmiddels wel sterk veranderd. Overheden zitten inmiddels met een aandeel van 59% ondertekende domeinnamen boven in de ranglijst. Dat is met name te danken aan de opname van DNSSEC in de ‘pas toe of leg uit’-lijst (ptolu) van het Forum Standaardisatie en de lancering van de (algemeen beschikbare) Internet.nl portal.
> Tabel met bevindingen, per sector.

		2017			2014		
Sectoren	**Categorieën** (klik voor details)	**Domeinen**	**Ondertekend**	**Percentage**	**Domeinen**	**Ondertekend**	**Percentage**
Financiële dienstverleners	Financials	278	44	16%	235	12	5%
	Banken	64	4	6%			
	Betalingsverkeer	54	9	17%			
	Verzekeraars	119	27	23%			
	Pensioenfondsen	194	58	30%	157	7	4%
	Pensioenorganisaties	14	5	36%	6	0	0%
	Gepensioneerden-organisaties	31	13	42%			
Publieke sector	Politiek	65	25	38%			
	Overheidsorganisaties	624	371	59%	655	73	11%
	Gemeenten	395	50	63%			
	ZBO's	69	20	29%			
	Toezichthouders	30	6	20%			
	Zorginstellingen	217	67	31%			
	Hoger onderwijs	89	18	20%	28	6	21%
	Wetenschappelijk onderzoek	152	52	34%	128	12	9%
	Onderzoeksorganisaties (NARCIS)	958	229	24%			
Internet en telecom	Telecom	6	2	33%	4	0	0%
	MVNO's	76	19	25%	96	18	19%
	Internet-providers	24	6	25%	27	2	7%
	Internet Service Providers	79	17	22%			
	Internet-infrastructuur	39	25	64%	42	16	38%
	AMS-IX leden	758	58	8%			
	NL-ix leden	593	121	20%			
Bedrijfsleven	Beursgenoteerde ondernemingen	107	13	12%	64	5	8%
	Nutsvoorzieningen	56	21	38%			
	Thuiswinkels	2065	611	30%	2044	480	23%
	Kranten	51	14	27%	45	12	27%

5 Internet en telecom

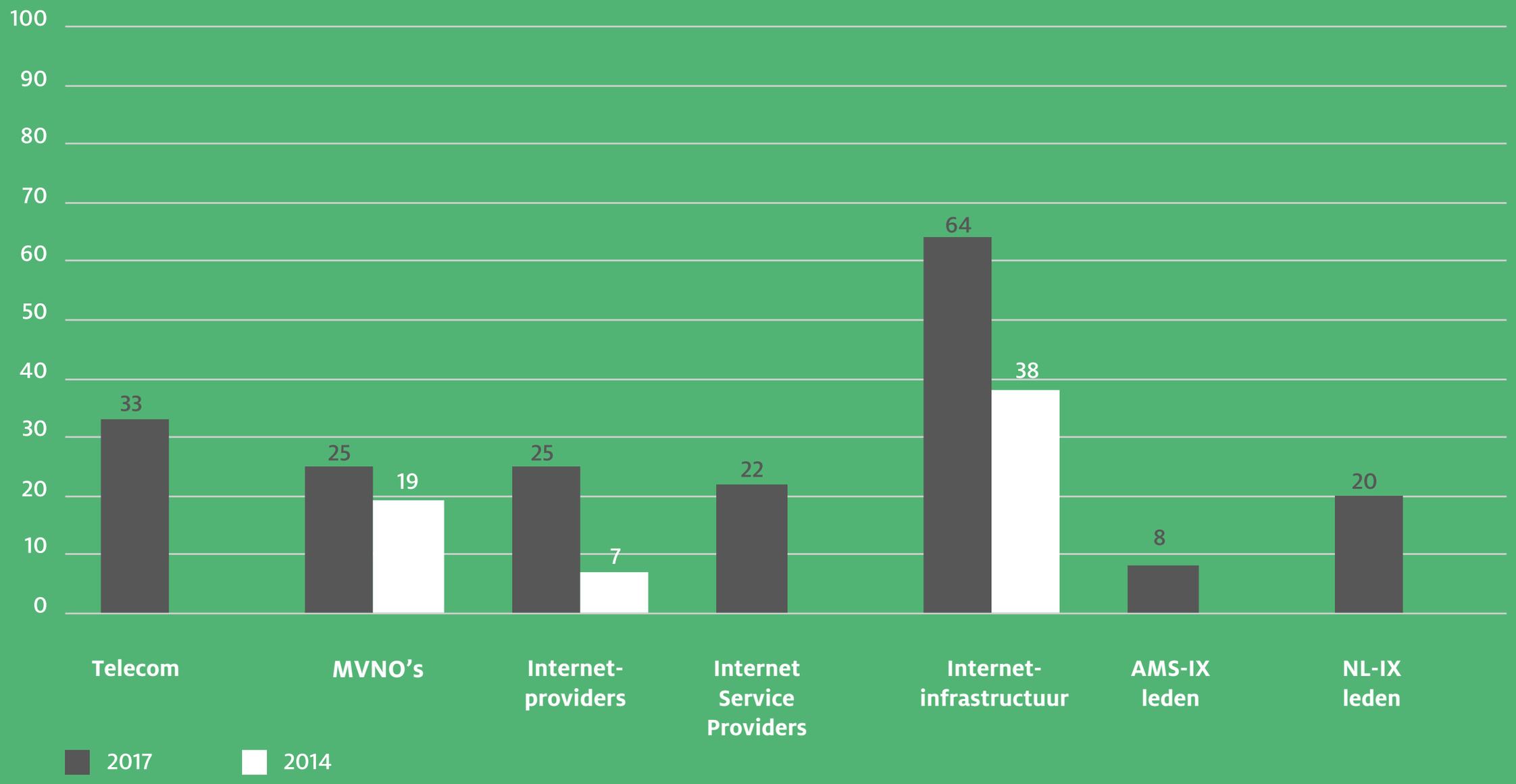
Alleen de specialisten die het Nederlandse internet ontwikkelen en onderhouden – waaronder ook SIDN – scoren met 64% hoger dan de overheid. De Internet-providers (IAP's) en Internet Service Providers (ISP's) zitten nu met respectievelijk 25% en 22% in de middenmoot, waar de IAP's twee-en-half jaar geleden nog maar 7% scoorden.

De grote ondernemingen verantwoordelijk voor de onderdelen van de Nederlandse digitale infrastructuur en de verbindingen met de rest van de wereld doen het echter slecht. Slechts een klein deel van deze bedrijven heeft zijn domeinnaam ondertekend.

Van de vier mobiele telecom-aanbieders (KPN, T-Mobile, Tele2 en Vodafone) heeft nog steeds geen een zijn domeinnaam ondertekend – die 33% is een vertekende statistiek omdat we hier ook RTV-zendmast-beheerder Alticom en toezichthouder Agentschap Telecom bij hebben gezet, en die hebben beide hun domeinnaam wel ondertekend.

Ook de ondernemingen verantwoordelijk voor de datatransport-backbone scoren opvallend laag: van de leden van de Amsterdam Internet Exchange (AMS-IX) en NL-ix knooppunten hebben respectievelijk maar 8% en 20% hun domeinnaam ondertekend. Dat wringt met name met de positionering van de Nederlandse digitale infrastrcutuur als de derde mainport [1, 2, 3] naast Schiphol en de Rotterdamse haven.
> Figuur 10: DNSSEC-ondertekend (in %)

Internet en telecom



Figuur 10: DNSSEC-ondertekend (in %)

6 Financiële dienstverleners

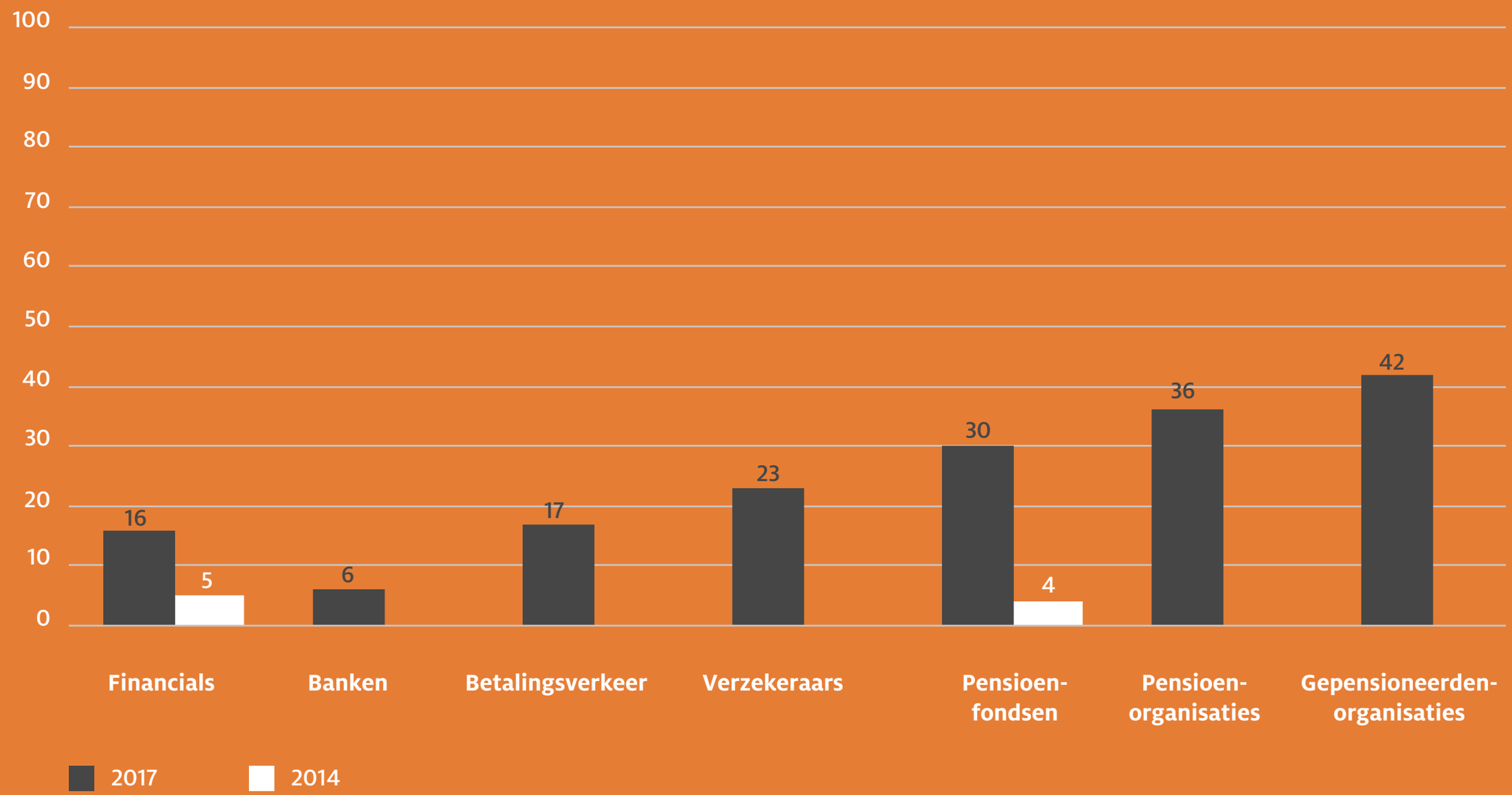
De banken deden het twee-en-half jaar geleden niet alleen het slechtst van allemaal, ze zijn in de tussentijd ook absoluut stil blijven staan. Slechts een enkeling (ASN, ASR, DHB en Interbank) heeft zijn domeinnaam ondertekend, en dat is exact dezelfde sitatie als toendertijd. De reactie van Betaalvereniging Nederland destijds – de technologie is nog niet volwassen genoeg en er zijn nog niet genoeg validerende Internet-providers – gaf al weinig hoop op verbetering.

Desondanks zijn wij van mening dat van alle onderzochte categorieën de banken de belangrijkste gebruikers van DNSSEC zouden moeten zijn. Met het opdoeken van de bankkantoren en het verminderen van het aantal pinautomaten is de online voordeur van de banken steeds belangrijker geworden. Bovendien hebben zij het meest van alle online bedrijven last van phishing, iets waar onder andere DNSSEC in combinatie met DKIM bescherming tegen kan bieden.

De collega's in verzekeringen en pensioenen hebben zich in de afgelopen twee-en-half jaar wel sterk weten te verbeteren, en doen op dit moment mee in de middenmoot.
> Figuur 11: DNSSEC-ondertekend (in %)

**) Uit de 900.000 meldingen die over de afgelopen jaren bij Fraudehelpdesk.nl zijn binnengekomen blijkt dat 70-80 procent van de phishing-mailberichten is gericht op de banken. Dit aandeel is over de jaren heen constant gebleven. Zo blijkt uit onderzoek van Elmer Lastdrager. Hij werkt bij de Universiteit Twente aan APATE, het systeem dat de meldingen van de Fraudehelpdesk verwerkt en analyseert. De bevindingen van Lastdrager worden gepubliceerd in zijn proefschrift dat later dit jaar verschijnt.*

Financiële dienstverleners



Figuur 11: DNSSEC ondertekend (in %)

7 Publieke sector

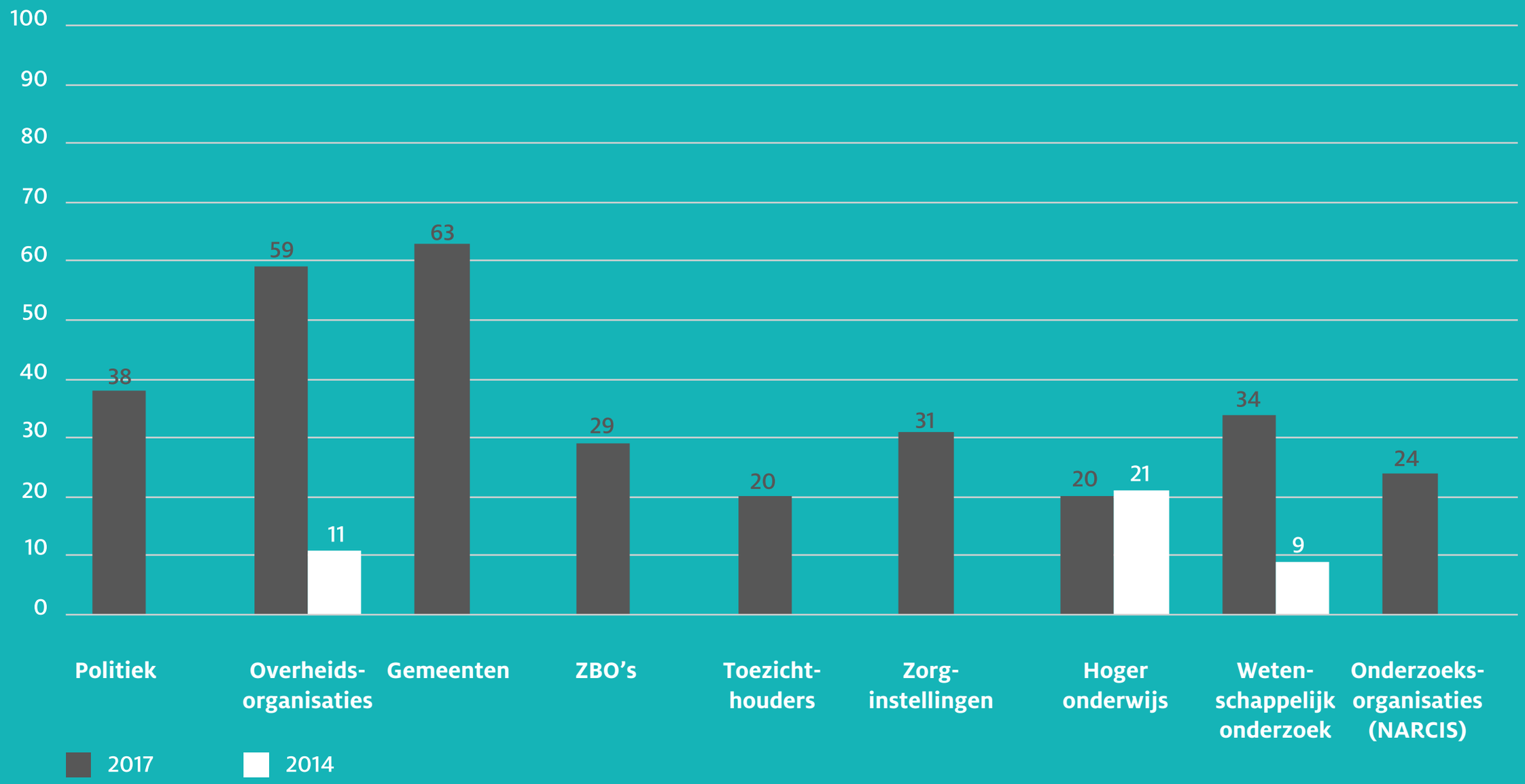
Hetzelfde geldt voor overheidsorganisaties. Zij bleven twee-en-half jaar geleden sterk achter bij de rest van de domeinnaamhouders, maar hebben inmiddels een veel betere positie ingenomen. Dat is duidelijk het gevolg van beleid op dit gebied. DNSSEC is vier jaar geleden op de 'pas toe of leg uit'-lijst (ptolu) van het Forum Standaardisatie gezet. Onlangs zijn STARTTLS en DKIM voor mail daar bij gekomen. Dat betekent dat overheidsorganisaties bij de vernieuwing van hun systemen min-of-meer verplicht zijn om deze standaarden te implementeren.

Daarnaast heeft het Forum Standaardisatie er vorig jaar de Internet.nl portal opgezet. Daar kan iedereen zijn eigen domeinnaam of die van anderen controleren op het gebruik van moderne en veilige internet-standaarden.

Naar aanleiding van berichtgeving over de slechte beveiliging van gemeentelijke sites heeft Minister Plasterk van Binnenlandse Zaken vorig jaar aangegeven dat alle Nederlandse gemeenten eind 2017 hun domeinnamen met DNSSEC moeten hebben beveiligd. Die aansporing heeft over de afgelopen maanden ook duidelijk geleid tot actie: inmiddels is maar liefst 63% van de gemeentelijke domeinnamen ondertekend.

Opvallende stijger in deze sector is ook de onderzoekswereld, waarvan het aandeel ondertekende domeinnamen van 9% naar 34% is gegroeid. SIDN heeft daar ook een belangrijke aanzet gegegeven door in de zomer van 2014 als onderdeel van de Campus Challenge vijf instellingen te helpen met hun DNSSEC-implementatie.
› Figuur 12: DNSSEC-ondertekend (in %)

Publieke sector



Figuur 12: DNSSEC-ondertekend (in %)

8 Bedrijfsleven

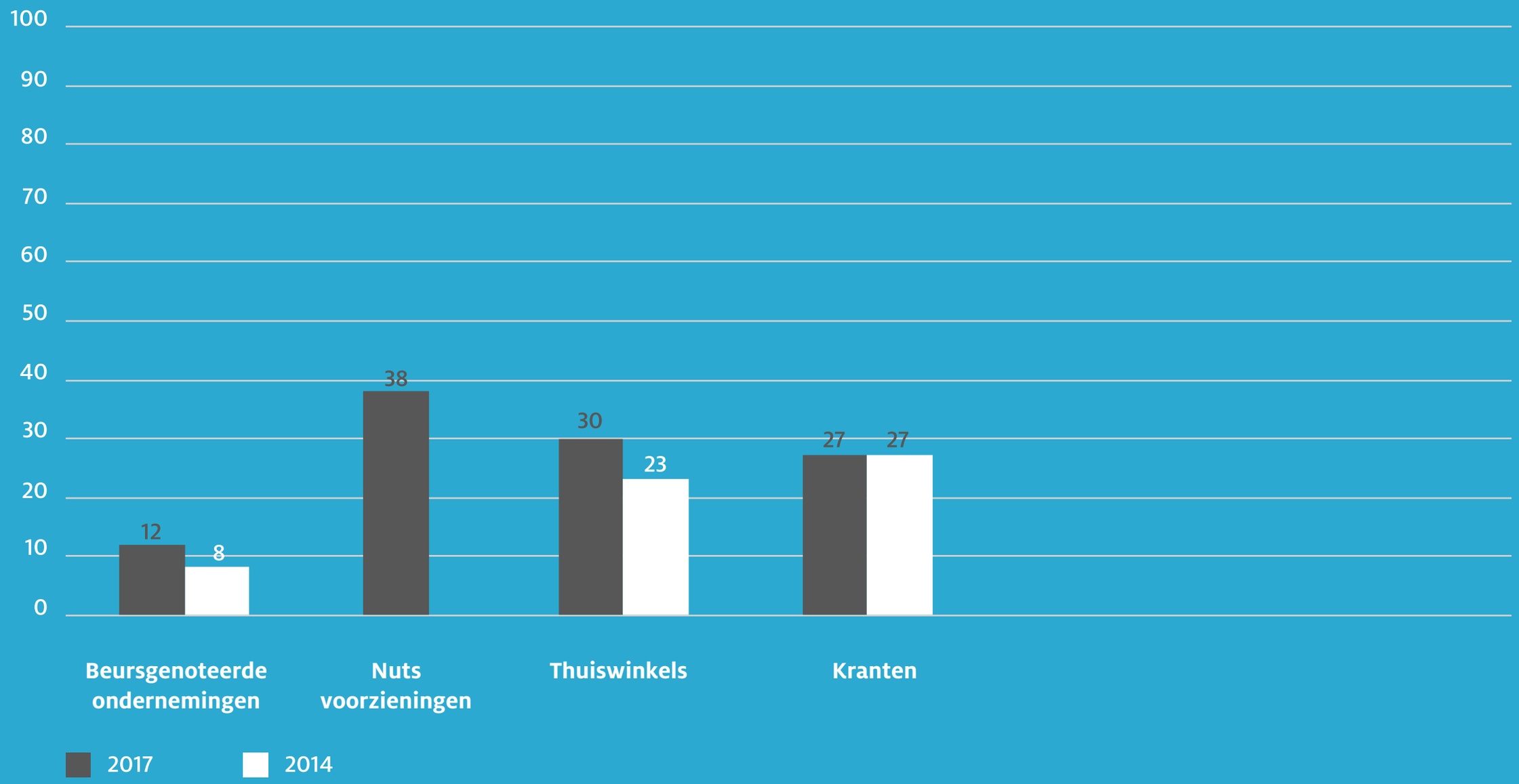
In het Nederlandse bedrijfsleven kruipt het aandeel ondertekende domeinnamen vooruit. Beursgenoteerde ondernemingen en thuiswinkels zijn er ietsje op vooruit gegaan. De kranten hebben de afgelopen twee-en-half jaar echter stilgestaan. Met een aandeel van 12% ondertekende domeinnamen doen de beursgenoteerde ondernemingen het nog steeds erg slecht.

De initiële razendsnelle groei bij de kleine bedrijven (thuiswinkels) is inmiddels afgevlakt. Die was destijds te danken aan de grote registrars die hun domeinen met honderdduizenden tegelijk ondertekenden, gedreven door de incentive-regeling van SIDN. Omdat veel van de kleine bedrijven hun site met alles erop en eraan bij een dienstverlener afnemen, liftten zij hier automatisch op mee.

Alle registrars met een dergelijk groot portfolio aan .nl-domeinen hebben DNSSEC inmiddels ingevoerd, waarmee ook die razendsnelle groei er niet meer is. Wat dat betreft heeft de integrale aanpak van SIDN met de incentive-regeling zijn werk gedaan. De huidige, meer gestage groei wordt vooral gedreven door middelgrote en kleine registrars en bedrijven, voor wie de implementatie van DNSSEC meestal onderdeel is van een upgrade van hun DNS-infrastructuur.

Grote ondernemingen in het algemeen, en banken en telecom-bedrijven in het bijzonder, staan bekend om hun traagheid van bewegen. Daarnaast zijn het veel meer dan andere organisaties gebruikers van Infoblox-appliances. De DNSSEC-implementatie van Infoblox is echter sterk verouderd, wat een aanvullende reden zou kunnen zijn voor grote ondernemingen om de ondertekening van hun domeinnamen uit te stellen.
> Figuur 13: DNSSEC-ondertekend (in %)

Bedrijfsleven



Figuur 13: DNSSEC-ondertekend (in %)

9 Conclusie

Globaal genomen is het aandeel ondertekende domeinnamen voor de onderzochte sectoren over de afgelopen twee-en-half jaar sterk gegroeid. Daarmee loopt de ontwikkeling in die segmenten waarvoor wij menen dat DNSSEC belangrijk is parallel aan de bredere trend. Wel blijven vrijwel al deze sectoren ver achter ten opzichte van het gemiddelde aandeel ondertekende domeinnamen (46%).

Zowel deze als de vorige meting laat bovendien grote verschillen zien tussen de verschillende sectoren. In het algemeen doen kleinere bedrijven, die meestal hun site met alles erop en eraan bij een dienstverlener afnemen, het (automatisch) veel beter dan de grote ondernemingen.

Duidelijke uitzonderingen, in tegenovergestelde zin, zijn de overheden en de banken. Overheidsorganisaties zitten inmiddels met een aandeel van 59% ondertekende domeinnamen in de top van de ranglijst. De banken daarentegen zijn als een van de weinige groepen volledig stil blijven staan. Een enkele uitzondering daargelaten wordt DNSSEC door deze bedrijven simpelweg niet ingezet om hun domeinnamen te beveiligen.

Deze laatste constatering is wat ons betreft reden tot zorg. Met het opdoeken van de bankkantoren en het verminderen van het aantal pinautomaten is de online voordeur van de banken steeds belangrijker geworden. Bovendien hebben zij het meest van alle online bedrijven last van phishing, iets waar onder andere DNSSEC in combinatie met DKIM bescherming tegen kan bieden.

Ook de uitkomsten voor de internet- en telecom-sector zijn teleurstellend. Waar de IAP's en ISP's nu voorzichtig meedoen in de middenmoot, scoren mobiele telecom-aanbieders en de ondernemingen verantwoordelijk voor de datatransport-backbone ronduit slecht.

Deze slechte score van de ondernemingen verantwoordelijk voor de onderdelen van de Nederlandse digitale infrastructuur en de verbindingen met de rest van de wereld staat in schril contrast met de positionering van het Nederlandse internet als de derde mainport naast Schiphol en de Rotterdamse haven.

Colofon

Dit is een verslag van een onderzoeksrapport dat is samengesteld door Offerman Consulting in opdracht van SIDN.
Aan dit verslag werkten mee:

Offerman Consulting
Adrian Offerman – Specialist journalist

SIDN
Nick Boerman – Business Intelligence Analist
Marco Davids – Research engineer
Marnie van Duijnhoven – Communicatiemanager

Lumen ontwerpersnetwerk
Ronald van Lit – Ontwerper
Eugène Heijblom – Ontwerper

Heb je vragen, mail dan naar
communicatie@sidn.nl

SIDN
Postbus 5022
6802 EA Arnhem
Meander 501
6825 MD Arnhem
T +31 (0)26 352 55 00
www.sidn.nl