FS-20181212.02A

Overheidsbreed Beleidsoverleg Digitaal Overheid

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Agendapunt 5d: Standaardisatie
Door: Forum Standaardisatie

---

1. Halfjaarlijkse meting informatie veiligheid (IV-) standaarden (eind september 2018)

OBDO-leden wordt gevraagd:

- Kennis te nemen van de stand van zaken van de adoptie van de Informatie Veiligheid standaarden (IV-standaarden).
- De adoptie van deze standaarden in uw organisatie/achterban te stimuleren, conform uw eerdere streefbeeldafspraken en het instellingsbesluit OBDO (art 4 lid 2).
- In de bijlage is meer informatie over de meting en de uitkomsten per organisatie te vinden.
  Call to action: U wordt gevraagd deze bijlage binnen uw organisatie/achterban te verspreiden (bijv. via CIO's, CTO's & CISO's), en aan te sturen op implementatie bij achterblijvers, bijvoorbeeld door agendering via de koepels. Het Forum Standaardisatie helpt daarbij desgewenst graag.

Waar gaat het over

Burgers en ondernemers moeten erop kunnen vertrouwen dat gegevensuitwisseling met de overheid en tussen overheden veilig verloopt. Hiervoor dienen overheden meerdere informatieveiligheidsstandaarden te implementeren. Recente phishing-incidenten waarin overheids e-mail en websites werden nagemaakt onderstrepen nogmaals het belang van overheidsbrede adoptie van deze standaarden. Het OBDO en zijn voorganger het Nationaal Beraad Digitale Overheid (NB) hebben daarom implementatieafspraken gemaakt over standaarden voor het beveiligen van mail en websites.

Het NB sprak begin 2016 de ambitie uit om in belang van veilige digitale berichtenuitwisseling een set van vijf informatieveiligheidstandaarden (IV-standaarden)[1] versneld te adopteren. Doel: eind 2017 zijn overheidswebsites en e-maildomeinen (waar relevant) beveiligd met behulp van de IV-standaarden. Aanvullend hierop zijn in het Nationaal Beraad verdergaande afspraken gemaakt over een set van standaarden voor het beveiligen van alle overheidswebsites met als deadline uiterlijk 2018.[2] Hier bovenop zijn in het OBDO van april 2018 aanvullende streefbeeldafspraken gemaakt over een set van standaarden voor het beveiligen van mail met als deadline uiterlijk 2019.[3] Er zijn dus drie streefbeeldafspraken, met verschillende deadlines.[4]

[1] Het betreft de standaarden DNSSEC voor domeinnaambeveiliging, TLS voor beveiligde verbindingen, DKIM en SPF voor anti-phishing en DMARC voor anti-phishing rapportages.
[2] Het betreft de standaarden HTTPS, HSTS en TLS conform de NCSC richtlijn voor de beveiligde verbindingen van websites.
[3] Het betreft de standaarden STARTTLS en DANE voor encryptie van mailverkeer tegen afluisteren. En het instellen van strikte policies voor de emailstandaarden SPF en DMARC.
[4] Voor aanvullende informatie over de afspraken zie: https://www.forumstandaardisatie.nl/thema/iv-meting-en-afspraken

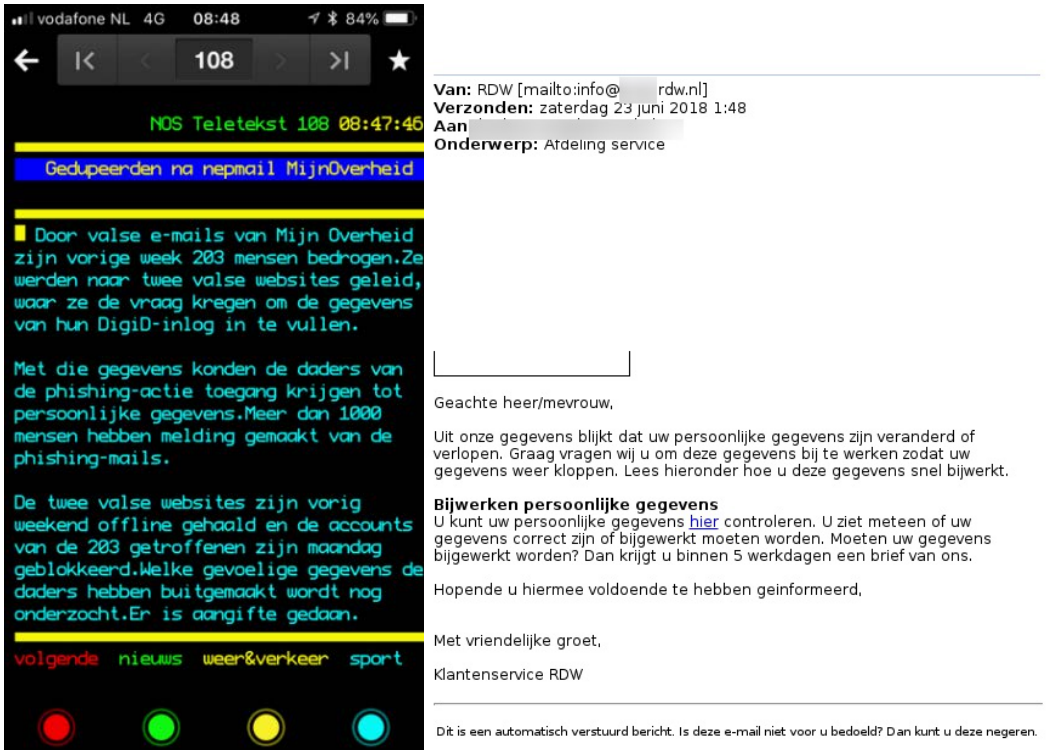
De resultaten

Om de voortgang bij te houden voert het Forum twee keer per jaar een IV-meting uit. De laatste meting dateert van september 2018, waarbij 563 domeinnamen zijn getoetst. Uit de meting van september 2018 blijkt dat de adoptie opnieuw is gegroeid.

Kijkende naar de eerste streefbeeldafspraak (deadline eind 2017) is de adoptie gestegen naar 87%. Ter vergelijking: begin dit jaar was het nog 80%. Voor de tweede streefbeeldafspraak (deadline eind 2018: op elke overheidssite het slotje (https) geconfigureerd conform NCSC advies) is de adoptie gestegen naar 85%, begin dit jaar was het 78%. Voor de derde streefbeeldafspraak (beveiliging tegen e-mail afluisteren & strenge configuratie e-mail standaarden) is de adoptie momenteel 59%. Hierover zijn geen eerdere gegevens beschikbaar.

De implementatie van de IV-standaarden loopt daarmee nog wel achter op het doel, namelijk 100% adoptie. Dit is met name het geval als we kijken naar de adoptie van de mailstandaarden. Zonder aanvullende campagnes, activiteiten en of verplichtingen zal zo goed als volledige adoptie eind 2019 lastig te realiseren zijn voor de mailstandaarden. Belangrijk is om per doelgroep te kijken naar welke standaarden extra aandacht nodig hebben en of er ‘quick wins’ zijn. Dat doet het Forum Standaardisatie graag met de koepels van de organisaties. Om voor de webstandaarden 100% adoptie te halen is het nodig om de achterblijvende organisaties individueel aan te spreken en te helpen. Daarnaast kan een wettelijke verplichting helpen om de laatste paar procent zo ver te krijgen dat ze de standaarden ondersteunen. De StasBZK heeft aangegeven dat hij voornemens is een dergelijke verplichting te gaan realiseren.

Meer informatie over de meting en de uitkomsten per organisatie is te vinden in onze forumnotitie, die als bijlage is toegevoegd. U wordt gevraagd deze binnen uw organisatie/achterban te verspreiden, en aan te sturen op implementatie bij eventuele achterblijvers.



Figuren: voorbeelden van phishingmails (en hun efffect), die met de toepassing en juiste (strenge) configuratie van de anti-phishing standaarden hadden kunnen worden bestreden.

2. Mutaties pas-toe-of-leg-uit lijst

Het OBDO stelt vast welke open standaarden in Nederland verplicht moeten worden toegepast bij de aanschaf en ontwikkeling van ICT: het zogenaamde *pas-toe-of-leg-uit* beleid. Ook kan het OBDO standaarden met meerwaarde voor de overheid aanbevelen zonder verplichting en adoptieadviezen voor open standaarden geven. Hiermee draagt het OBDO bij aan de veiligheid, interoperabiliteit en leveranciersonafhankelijkheid van de digitale overheid.

De volgende standaarden liggen ter besluitvorming voor aan het OBDO om vastgesteld te worden als verplichte (pas toe of leg uit) of als aanbevolen standaarden:

a) [Hamerstuk] Actualisering versie internet veiligheidstandaard

Burgers en bedrijven moeten veilig kunnen communiceren met de overheid via e-mail of websites. Overheden moeten ook onderling veilig over het Internet kunnen communiceren. Een van de meest fundamentele open standaarden op de pas-toe-of-leg-uit-lijst, TLS, zorgt voor veilige verbindingen over het Internet. TLS is een onmisbare maar ook complexe standaard waarvan verschillende versies naast elkaar in gebruik zijn en die verschillende configuraties toelaat. Het Nationaal Cyber Security Centrum (NCSC) adviseert openbaar regelmatig over het correcte gebruik van TLS.

Om hackers en criminelen voor te blijven publiceerde de beheerder van de standaard dit jaar een nieuwe versie van TLS. Na een zorgvuldige toetsingsprocedure adviseert Forum Standaardisatie om deze nieuwe versie 1.3 op de pas-toe-of-leg-uit-lijst te plaatsen en de ook nog veilige versie 1.2 te behouden als terugval-versie voor compatibiliteit met oudere systemen. Op aandringen van vele organisaties waaronder het NCSC adviseert Forum Standaardisatie om de oudere versies 1.0 en 1.1 niet meer als terugval-opties aan te bevelen. Deze versies worden dan ook van de lijst verwijderd.

Het volledige Forumadvies is te vinden op de website van het Forum Standaardisatie: https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20181010.3A%20Forumadvies%20TLS%201.3..pdf

Beslispunt [Hamerstuk]:	Het OBDO stemt in met (i) plaatsing van versie 1.3 van de internet veiligheid standaard TLS op de pas-toe-of-leg-uit-lijst met behoud van versie 1.2 als terugval-optie (ii) verwijdering van versies 1.0 en 1.1 van TLS van de pas-toe-of-leg-uit-lijst als terugval-opties

b) [Hamerstuk] Actualisatie versie toegankelijkheidstandaard

Sinds 1 juli 2018 is het *Tijdelijk besluit toegankelijkheid digitale overheid* van kracht. Het Tijdelijk besluit schrijft voor dat online informatie van de overheid in 2020 moet voldoen aan de Europese toegankelijkheidsnorm (EN 301 549). Door de wettelijke verplichting zou de Europese norm van de is het ‘pas toe of leg uit’ beleid niet meer van toepassing. Toch adviseert Forum Standaardisatie om de norm tot tenminste 2019 op de pas-toe-of-leg-uit lijst te laten staan. Zodoende moet de toegankelijkheidsnorm voor 2020 al tenminste worden toegepast bij nieuwe investeringen in overheidswebsites.

Europa publiceert voor het einde van het jaar een nieuwe versie 2.1.2 van de Europese norm die per direct in de Nederlandse wet wordt overgenomen. Forum Standaardisatie adviseert om de versie van EN 301 549 op de pas-toe-of-leg-uit lijst hiermee gelijk te laten lopen.

Meer details zijn te vinden in de oplegnotitie Lijsten voor de vergadering van het Forum Standaardisatie van 10 oktober 2018: https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20181010.3%20Oplegnotitie%20Lijsten%20Open%20Standaarden.pdf

Beslispunt [Hamerstuk]:	Het OBDO stemt in met (i) Handhaving van de wettelijk verplichte Europese toegankelijkheidsnorm EN 301 549 op de pas-toe-of-leg-uit lijst tot september 2019 (ii) Gelijkschakeling van de versie van EN 301 549 op de pas-toe-of-leg-uit lijst met de versie waar het Tijdelijk besluit toegankelijkheid digitale overheid naar verwijst

c) [Hamerstuk] Functioneel toepassingsgebied e-mail veiligheidstandaard

De overheid moet inkomende en uitgaande e-mail berichten beschermen tegen onderschepping en manipulatie, bijvoorbeeld door aanvallers die valse WiFi hotspots inzetten. Hiervoor verplicht de overheid het gebruik van standaarden (STARTTLS en DANE) die in combinatie beschermen tegen dit soort aanvallen. In 2016 besloot het Nationaal Beraad Digitale Overheid om deze standaarden voor *inkomende* e-mail te verplichten. Een verplichting voor *uitgaande* e-mail werd voorbarig gevonden omdat de marktondersteuning voor uitgaande mail toen nog achterliep.

Het marktaanbod voor deze standaarden is inmiddels dusdanig verbeterd dat een verplichting voor uitgaande e-mail nu werkbaar en wenselijk is voor de overheid. Na een zorgvuldige toetsingsprocedure adviseert het Forum Standaardisatie daarom om het functioneel toepassingsgebied van STARTTLS en DANE uit te breiden naar zowel inkomende als uitgaande e-mail.

Het volledige Forumadvies is te vinden op de website van het Forum Standaardisatie: https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20181010.3C%20Forumadvies%20uitbreiding%20toepassingsgebied%20STARTTLS%20en%20DANE..pdf

Beslispunt [Hamerstuk]:	Het OBDO stemt in met de uitbreiding van het functioneel toepassingsgebied van de e-mail veiligheid standaarden tegen afluisteren STARTTLS en DANE op de pas-toe-of-leg-uit lijst naar zowel ontvangende als verzendende e-mail servers.

d) [Hamerstuk] Verwijdering standaard voor gegevensuitwisseling in de afvalverwerking

In de (gemeentelijke) afvalverwerking zorgen open ICT standaarden voor betere uitwisselbaarheid van gegevens en leveranciersonafhankelijkheid. De hiervoor verplichte standaard (STOSAG 1.0) blijkt niet meer actueel te zijn door een privacy probleem. Met de chips op afvalcontainers zouden derden persoonsgegevens en gebruiksgegevens kunnen uitlezen van de bewoners van een gemeente.

De beheerder van de standaard (STOSAG) heeft het Forum Standaardisatie niet uit eigen beweging op deze situatie gewezen, en heeft ondanks herhaalde contactpogingen geen geactualiseerde versie van de standaard aangemeld. Na zorgvuldige toetsingsprocedure adviseert het Forum Standaardisatie om STOSAG 1.0 daarom te verwijderen van de pas-toe-of-leg-uit lijst.

Het volledige Forumadvies is te vinden op de website van het Forum Standaardisatie: https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20181010.3D%20Forumadvies%20%20verwijdering%20STOSAG%201.0.pdf

Beslispunt [Hamerstuk]:	Het OBDO stemt in met de verwijdering van de afvalverwerking informatie uitwisselingstandaard STOSAG 1.0 van de pas-toe-of-leg-uit lijst.

e) [Hamerstuk] Aanbeveling Linked Data standaard

De overheid publiceert in toenemende mate open data. Ook gebruikt de overheid steeds meer open data in analytische processen, bijvoorbeeld bij fraudebestrijding en bij het verzamelen van statistieken. Het koppelen van open datasets kan informatie van toegevoegde waarde opleveren. Daarbij zijn de kwaliteit van de data en de kwaliteit van de koppeling wel van cruciaal belang.

De zogenaamde *Linked Data* standaarden zorgen ervoor dat je datasets met elkaar kan verbinden. Voor het beheren van de kwaliteit van Linked Data verzamelingen is recent een open standaard gepubliceerd (SHACL). Na een zorgvuldige toetsingsprocedure adviseert het Forum Standaardisatie om SHACL als opkomende standaard op te nemen op de lijst aanbevolen standaarden.

Het volledige Forumadvies is te vinden op de website van het Forum Standaardisatie: https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20181010.3F%20Forumadvies%20SHACL.pdf

Beslispunt [Hamerstuk]:	Het OBDO stemt in met de plaatsing van de Linked Data standaard SHACL op de lijst aanbevolen standaarden

f) [Hamerstuk] Aanbeveling standaard voor extra e-mail veiligheid

Een kleine groep overheidsorganisaties vereist een hoog niveau van e-mail veiligheid waarbij de integriteit van een bericht op het hele pad van verzender naar ontvanger gegarandeerd wordt, ook binnen de organisatie zelf. Voor deze organisaties bieden de verplichte e-mail veiligheidstandaarden (waaronder de hierboven bij punt b genoemde standaarden) onvoldoende beveiliging. Standaarden zoals S/MIME die dit hogere veiligheidsniveau wel bieden zijn ook aanzienlijk complexer en kostbaarder in implementatie.

Na een zorgvuldige toetsingsprocedure adviseert het Forum Standaardisatie om S/MIME aan te bevelen voor organisaties waarvoor de integriteit van e-mails van fundamenteel belang is en de kosten tegen de baten opwegen.

Meer details zijn te vinden in de oplegnotitie Lijsten voor de vergadering van het Forum Standaardisatie van 10 oktober 2018:
https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20181010.3%20Oplegnotitie%20Lijsten%20Open%20Standaarden.pdf

Beslispunt [Hamerstuk]:	Het OBDO stemt in met de plaatsing van S/MIME op de lijst aanbevolen standaarden voor organisaties die een hoog niveau van veiligheid vereisen voor de integriteit van e-mails.

notitie

Forum Standaardisatie

www.forumstandaardisatie.nl

info@forumstandaardisaties.nl

Bureau Forum Standaardisatie

gehuisvest bij Logius

Postadres

Postbus 96810

2509 JE Den Haag

Bezoekadres

Wilhelmina van Pruisenweg 52

2595 AN Den Haag

Bij bezoek aan Logius is legitimatie

FORUM STANDAARDISATIE 10 oktober 2018

IV-meting september 2018

Van:	Stuurgroep open standaarden
Aan:	Forum Standaardisatie

Voor u liggen de resultaten uit de meting informatieveiligheidsstandaarden van september 2018 (hierna: IV-meting). De meting heeft betrekking op een aantal informatieveiligheidsstandaarden waarvoor, in aanvulling op het 'pas toe of leg uit' beleid, overheidsbrede streefbeeldafspraken met uiterlijke implementatiedata zijn gemaakt door het Nationaal Beraad en het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO).

Sinds februari 2016 voert Forum Standaardisatie twee keer per jaar een IV-meting uit naar de voortgang van de streefbeeldafspraken. In 2,5 jaar tijd is voor de standaarden van de eerste streefbeeldafspraak de gemiddelde adoptiegraad onder overheden toegenomen van 35% naar meer dan 80%. Na het publiceren van de eindmeting begin 2018 heeft het OBDO ingestemd met aanvullende streefbeeldafspraken.

De voorliggende meting omvat de afgeronde streefbeeldafspraak (eind 2017) om te zien welke progressie de groep achterblijvers maakt, en daarnaast de twee lopende streefbeeldafspraken (eind 2018 en eind 2019). Ook is de lijst met de te toetsen domeinnamen ten opzichte van de vorige meting geactualiseerd. In onderliggende notitie vindt u meer informatie over de afspraken en de uitkomsten uit de meting.

Ter besluitvorming
U wordt gevraagd in te stemmen met:

A. De resultaten uit de IV-meting van september 2018 en het voorleggen hiervan aan OBDO;
B. De resultaten uit de IV-meting in uw achterban uit te zetten en onder de aandacht te brengen van met name de achterblijvende organisaties.
C. Te bespreken welke aanvullende acties kunnen worden ondernomen, om de groei te versnellen van die standaarden waarvan de groei vooralsnog onvoldoende is, zodat de afgesproken streefbeelden gehaald worden.

FS-20181212.02A

Halfjaarlijkse meting **Informatieveiligheidsstandaarden** Forum Standaardisatie

= September 2018 =

Achtergrond

Sinds 2015 biedt het Platform Internetstandaarden[1] de mogelijkheid om via de website Internet.nl domeinen te toetsten op het gebruik van een aantal moderne internetstandaarden, waaronder een aantal informatieveiligheidsstandaarden, die op de 'pas toe of leg uit'-lijst van Forum Standaardisatie staan. In datzelfde jaar is Forum Standaardisatie gestart om met behulp van Internet.nl een halfjaarlijkse meting van de adoptiegraad van informatieveiligheidsstandaarden voor overheidsdomeinen (web en e-mail) uit te voeren.

Die metingen hebben ertoe geleid dat het Nationaal Beraad in februari 2016 de ambitie uitsprak deze standaarden versneld te willen adopteren[2]. Dit betekent concreet dat voor deze standaarden niet het tempo van 'pas toe of leg uit' wordt gevolgd (d.w.z. wachten op een volgend investeringsmoment en dan de standaarden implementeren) maar dat actief wordt ingezet op implementatie van de standaarden op de kortere termijn[3].

De eerste streefbeeldafspraak is eind 2017 afgelopen. Begin 2018 is een eindmeting voor deze afspraak gepubliceerd. Ondanks een grote stijging de afgelopen twee jaar was volledige adoptie nog niet bereikt. Daarom zijn deze afspraken in april 2018 herbevestigd en aangevuld door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO), de opvolger van het Nationaal Beraad. De nieuwe meting is daarom uitgebreider (meer standaarden) dan voorgaande metingen. Daarnaast was het een goed moment om de lijst met de te toetsen domeinnamen te herijken en is besloten om het tijdstip van meten beter te laten aansluiten op de bestaande overlegcycli.

Om welke standaarden gaat het

Het Nationaal Beraad en het OBDO hebben bovengenoemde afspraken gemaakt met betrekking tot de volgende standaarden.[4]

REALISATIEDATUM	**WELKE STANDAARD GEADOPTEERD**
uiterlijk EIND 2017	TLS/HTTPS: beveiligde verbindingen van websites DNSSEC: domeinnaambeveiliging SPF: anti-phishing van email DKIM: anti-phishing van email DMARC: anti-phishing van email
uiterlijk EIND 2018	HTTPS, HSTS en TLS conform de NCSC richtlijn (externe link): beveiligde verbindingen van alle websites
uiterlijk EIND 2019	STARTTLS en DANE: encryptie van mailverkeer SPF en DMARC: het instellen van strikte policies voor deze emailstandaarden.

[1] Platform Internet Standaarden is een gezamenlijk initiatief van de Internetgemeenschap en de Nederlandse overheid (Forum Standaardisatie, het Ministerie van Economische Zaken en Klimaat, en NCSC). Zie https://internet.nl/about/

2 http://www.binnenlandsbestuur.nl/digitaal/nieuws/nationaal-beraad-wil-sneller-moderne-e.9540822.lynkx

[3] Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. De halfjaarlijkse IV-meting is ook onderdeel van de jaarlijkse Monitor Open standaarden beleid.

[4] Voor meer informatie ga naar: https://www.forumstandaardisatie.nl/thema/iv-meting-en-afspraken

Om welke domeinnamen gaat het

In totaal zijn in deze meting 563 (vorige keer 530) domeinnamen van overheidsorganisaties getoetst, bestaande uit:

- Domeinen die horen bij de deelnemers van het OBDO;
- De domeinen die horen bij voorzieningen van de basisinfrastructuur (GDI);
- De 30 best bezochte domeinen van Rijksoverheden (en uitvoerders);
- De domeinen van de andere overheidsorganisaties die direct of indirect vertegenwoordigd zijn in het OBDO, zoals:
    - Uitvoerders (de Manifestpartijen);
    - Partijen die behorend tot Klein LEF;
    - Gemeenten;
    - Provincies;
    - Waterschappen.

Bij de selectie van de relevante domeinnamen is telkens gekozen voor het hoofdomein waarop de website van de overheidsorganisatie bereikbaar is. Daarnaast is gekozen voor het hoofdomein dat de desbetreffende overheidsorganisatie gebruikt voor e-mail (vaak dezelfde als voor web). Bij uitzondering zijn ook subdomeinen geselecteerd, bijvoorbeeld voor bekende inlogportalen of op verzoek van de beheerder.

Ten opzichte van de vorige meting is de lijst geactualiseerd. Hierdoor zijn er nieuwe domeinnamen bijgekomen en zijn niet-relevante domeinnamen verwijderd. De reden hiervoor kan verschillen, bijvoorbeeld omdat er een gemeentelijke herindeling heeft plaatsgevonden of dat er waterschappen zijn samengevoegd. Ook is de lijst met best bezochte domeinnamen aangepast en zijn alle organisaties uit de Manifestgroep en Klein Lef toegevoegd.

Het betreft echter nog steeds een selectie van domeinnamen. De lijst is niet volledig en kan dat ook niet zijn omdat de overheid momenteel geen overzicht heeft over alle domeinnamen. De gemeten domeinen zijn bij lange na niet alle domeinen waar het OBDO direct en indirect voor verantwoordelijk is, zo beheert het ministerie van AZ al meer dan 6000 domeinnamen. Een 100% score op deze domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn tegen bijvoorbeeld phishing. Mocht uwer inziens een relevante domeinnaam ontbreken dan verzoeken we om deze aan ons door te geven.

Hoe wordt gemeten

De meting geeft de stand van zaken weer op de peildatum 25 september 2018. De meting laat zien of op een domeinnaam de standaarden worden toegepast.

De meting wordt uitgevoerd middels een bulktoets via de API van Internet.nl. Voor de web-standaarden wordt het hoofddomein getoetst met de toevoeging www. (dus: www.forumstandaardisatie.nl), omdat het gebruikelijk is dat de website daarop bereikbaar is. Voor de maildomeinen wordt getoetst zonder enig voorvoegsel omdat dat doorgaans gebruikt wordt als e-maildomein (dus @forumstandaardisatie.nl).

Op Internet.nl kun je eenvoudig testen of je website of e-mail een aantal moderne internetstandaarden ondersteunen, ook de standaarden waarover streefbeeldafspraken zijn gemaakt zijn onderdeel van de test. Overigens heeft de score die een domeinnaam op Internet.nl kan halen (namelijk max. 100%) geen relatie met het resultaat uit deze meting aangezien wij toetsen op een subset van de standaarden. De website Internet.nl is een initiatief van het Platform Internetstandaarden. In het platform participeren verschillende partners uit de internetgemeenschap (Internet Society, RIPE NCC, SIDN en SURFnet) en Nederlandse overheid (Forum Standaardisatie, het Ministerie van Economische Zaken en Klimaat, en

NCSC). Het uitgangspunt is dat Internet.nl de adviezen van Forum Standaardisatie en NCSC met betrekking tot de Internetstandaarden volgt.

De meting geeft geen inzicht in het risiconiveau van een bepaald domein. Zo is het aannemelijk dat de aantrekkelijkheid van misbruik hoger is bij domeinen van grote uitvoerders (zoals *phishing* met aanmaningen) dan bij domeinen van kleine gemeenten.

In de meting wordt alleen gekeken naar de toepassing van standaarden op domeinnamen. Er wordt in de meting (nog) niet gekeken naar de andere ontvangende kant, bijvoorbeeld de controle op DMARC door bijvoorbeeld e-mailproviders van consumenten, en validatie van DNSSEC en DANE.

Over de standaarden

Er worden zowel web- als mailstandaarden gemeten. Hieronder per standaard een korte uitleg over wat deze doet. Overigens is meer (technische) informatie over wat er wordt getoetst te vinden op Internet.nl.

Web-standaarden

Wij meten het gebruik van de beveiligingsstandaarden voor het web ook op domeinen die alleen gebruikt worden voor mail omdat dit vaak wel domeinnamen zijn die re-directen naar het hoofddomein. Ook hiervoor moet de standaarden juist worden toegepast en burgers weten vaak niet hoe deze domeinen worden gebruikt. Als je re-directs toepast dan moeten ook de doorverwijzende domeinen met HTTPS beveiligd zijn, anders is de beginschakel niet veilig en daarmee is ook de gehele keten onveilig. Dit geldt ook als een zogenaamde 'parking page' wordt getoond. Alleen als een geregistreerd domein geen webpagina bevat dan is HTTPS niet nodig (en niet mogelijk).

DNSSEC	Domain Name System (DNS) is het registratiesysteem van namen en bijbehorende internetnummers en andere domeinnaaminformatie. Het is vergelijkbaar met een telefoonboek. Dit systeem kan worden bevraagd om namen naar nummers te vertalen en omgekeerd. Er is getest of de domeinnaam ondertekend is met DNSSEC, zodat de integriteit van de DNS-informatie is beschermd. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
TLS	Als een bezoeker een onbeveiligde HTTP-verbinding heeft met een website, dan kan een kwaadwillende eenvoudig gegevens onderweg afluisteren of aanpassen, of zelfs het contact volledig overnemen. Getest wordt of TLS is toegevoegd aan HTTP om de verbinding te beveiligen. Op Internet.nl heet deze subtest 'HTTPS available'. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
TLS cf. NCSC	We maken een onderscheid tussen 'TLS' en 'TLS conform NCSC'. In het eerste geval wordt gebruik gemaakt van TLS en in het tweede geval is TLS bovendien zodanig geconfigureerd dat deze voldoet aan de aanbevelingen van het Nationaal Cyber Security Center (NCSC)[5]. Zodat de vertrouwelijkheid, de authenticiteit en integriteit van een bezoek aan een website is gegarandeerd. De streefbeeldafspraak is om hier voor 2019 aan te voldoen.
HTTPS	Er wordt getest of je webserver bezoekers automatisch doorverwijst van HTTP naar HTTPS op dezelfde domeinnaam óf dat deze ondersteuning biedt voor alleen HTTPS en niet

[5] Zie https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html. Een wijziging ten opzichte van de vorige meting is dat in de huidige meting ook de vertrouwensketen van het certificaat wordt meegenomen in de test voor TLS conform NCSC.

	voor HTTP. Op Internet.nl heet deze subtest 'HTTPS Redirect'. De streefbeeldafspraak is om hier voor 2019 aan te voldoen.
HSTS	HSTS zorgt ervoor dat een browser eist dat een website altijd HTTPS blijft gebruiken na het eerste contact over HTTPS. Dit helpt voorkomen dat een derde -bijvoorbeeld een kwaadaardige WiFi hotspot- een browser kan omleiden naar een valse website. Door HTTPS samen met HSTS te gebruiken wordt het gebruik van beveiligde verbindingen zoveel mogelijk afgedwongen. De streefbeeldafspraak is om hier voor 2019 aan te voldoen.

Mailstandaarden

Wij meten het gebruik van e-mailbeveiligingsstandaarden ook op domeinen waarvan een organisatie geen e-mail verstuurt. Dit is relevant omdat ook die domeinen worden misbruikt (burgers weten vaak niet dat deze domeinen niet door de organisatie worden gebruikt), en juist domeinen waarvandaan niet gemaild wordt, makkelijk kunnen worden geblokkeerd met behulp van SPF en DMARC (met de policies –all en p=reject). =

DMARC	Met DMARC kan een e-mailprovider kenbaar maken hoe andere (ontvangende) mailservers om dienen te gaan met de resultaten van de SPF- en/of DKIM-controles van ontvangen e-mails. Dit gebeurt door het publiceren van een DMARC beleid in het DNS-record van een domein. In deze test wordt alleen gekeken of DMARC beschikbaar is, niet of er beleid is ingesteld. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
DMARC Policy	Zolang er geen beleid is ingesteld weet de ontvanger nog niet wat te doen met verdachte e-mail. De configuratie moet op orde zijn. (Opm: Actieve policies zijn ~all en –all voor SPF, en p=quarantine en p=reject voor DMARC) Er wordt gecontroleerd of de syntax van de DMARC-record correct is en of deze een voldoende strikte policy bevat. De streefbeeldafspraak is om hier voor 2020 aan te voldoen
DKIM	Met DKIM kunnen e-mailberichten worden gewaarmerkt. De ontvanger van een e-mail kan op die manier controleren of een e-mailbericht écht van de afzender afkomstig is en of het bericht onderweg ongewijzigd is gebleven. Getest wordt of de domeinnaam DKIM ondersteunt. Voor non-mail domeinen waar dit goed is ingesteld heeft DKIM verder geen toegevoegde waarde. In de meting wordt dit weergegeven middels de score "NVT" (niet van toepassing) voor DKIM. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF	SPF heeft als doel spam te verminderen. SPF controleert of een verzendende mailserver die e-mail namens een domein wil versturen, ook daadwerkelijk gerechtigd is om dit te mogen doen. Getest wordt of de domeinnaam een SPF-record heeft. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF Policy	Aanvullend op bovenstaande test wordt gecontroleerd of de syntax van de SPF-record geldig is en of deze een voldoende strikte policy bevat om misbruik van het domein door phishers en spammers tegen te gaan. De streefbeeldafspraak is om hier voor 2020 aan te voldoen.

STARTTLS	STARTTLS in combinatie met DANE gaan het afluisteren of manipuleren van mailverkeer tegen. STARTTLS maakt het mogelijk om transportverbindingen tussen e-mailservers op basis van certificaten met TLS te beveiligen. Er wordt getest of de ontvangende mailservers (MX) ondersteuning bieden voor STARTTLS. De streefbeeldafspraak is om hier voor 2020 aan te voldoen. Als er geen mailservers aanwezig is voor het domein dan wordt dit weergeven met NVT. Dit geldt ook voor STARTTLS CF. NCSC, DANE en DNSSEC MX.
STARTTLS CF. NCSC[6]	Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies van het TLS en verschillende versleutelingsstandaarden (ciphers). Aangezien niet alle versies en combinaties als voldoende veilig worden beschouwd, is het belangrijk om hierin de juiste keuze te maken en ook regelmatig te controleren of de gebruikte instellingen nog veilig zijn. Getest wordt of STARTTLS is geconfigureerd zoals door het NCSC is aanbevolen. De streefbeeldafspraak is om hier voor 2020 aan te voldoen.
DANE	DANE, dat voortbouwt op DNSSEC, zorgt er in combinatie met STARTTLS voor dat een verzendende e-mailserver de authenticiteit van een ontvangende e-mailserver kan controleren en het kan het gebruik van TLS bovendien afdwingen. Getest wordt of de nameservers van de mailservers één of meer TLSA-records voor DANE bevatten. De streefbeeldafspraak is om hier voor 2020 aan te voldoen
DNSSEC MX	DNSSEC is een randvoorwaarde voor het instellen van DANE. Daarom wordt getest of de domeinnamen van de mailservers (MX) ondertekend zijn met DNSSEC. Dit in het kader van de streefbeeldafspraak om voor 2020 STARTTLS en DANE te ondersteunen.

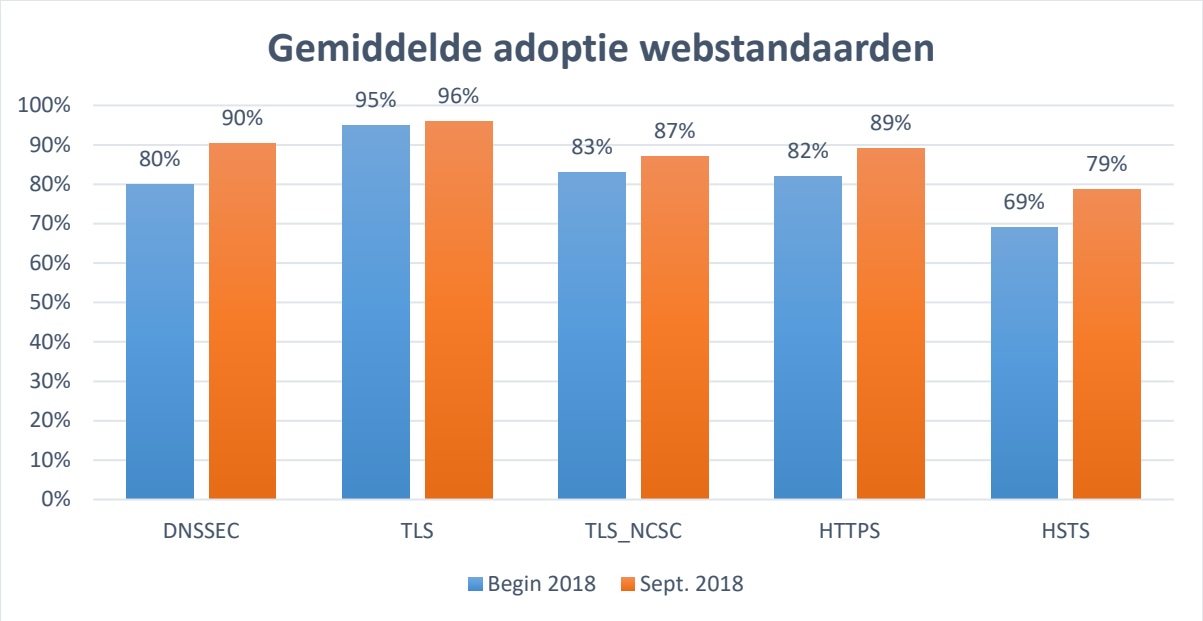
Resultaten meting september 2018

Eind augustus 2018 heeft het Bureau Forum Standaardisatie een eerste meting uitgevoerd, de resultaten zijn voorgelegd aan een aantal koepelorganisaties en stakeholders. Op 25 september 2018 heeft het Bureau Forum Standaardisatie de definitieve IV-meting uitgevoerd. Aangezien de eerste streefbeeldafspraak van het Nationaal Beraad afliep op 31 december 2017, is deze meting anders dan voorgaande metingen. Er zijn nieuwe resultaatafspraken toegevoegd en de te toetsten domeinnamen zijn aangepast. Dit maakt vergelijkbaarheid met de eerdere metingen moeilijker, ook omdat voor sommige standaarden geen eerdere cijfers beschikbaar zijn. Aan de hand van een aantal grafieken wordt de stand van zaken met betrekking tot adoptie toegelicht. De individuele resultaten van de test zijn te vinden in de bijlage.

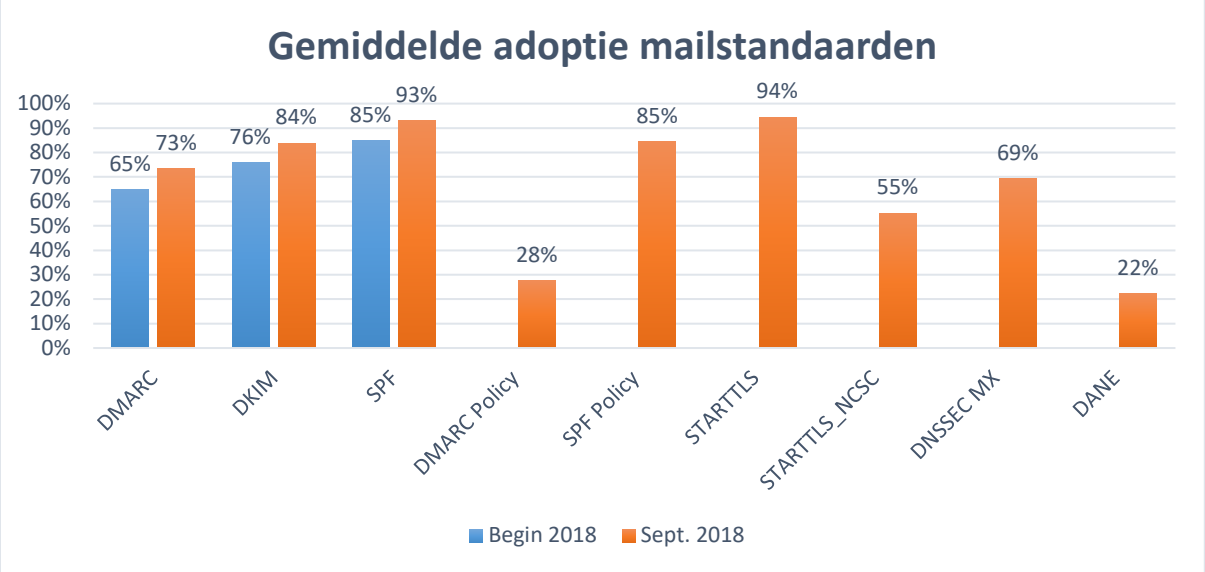
Per standaard

De onderstaande grafiek toont de adoptiestatus van de individuele standaarden voor zowel de webstandaarden als de mailstandaarden. Daar waar mogelijk is er een vergelijking gemaakt met de voorgaande meting.

[6] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html



Voor de standaarden uit de eerdere metingen (DNSSEC, TLS en TLS cf NCSC) zien we dat de groei nog steeds doorzet, met DNSSEC als uitschieter met 10 procentpunten naar 90%. Wel valt op dat de adoptie van TLS niet tot nauwelijks meer stijgt. Hiervoor is een 'één op één' benadering nodig om de 100% te halen. Van de standaarden met als streefdatum uiterlijk 2018 zien we dat HTTPS en TLS cf NCSC een hoge adoptiegraad hebben terwijl HSTS nog wat achterblijft met 79%, maar wel groeit.



Voor de standaarden uit de eerdere metingen (DMARC, DKIM en SPF) zien we dat de groei nog steeds goed doorzet. DMARC blijft, ondanks een stijging van 8 procentpunten, nog wel achter met 73%. Dat deze groei zich doorzet is positief aangezien het risico bestaat dat door het aflopen van de resultaatafspraak de aandacht voor het gebruik van de standaard afneemt.

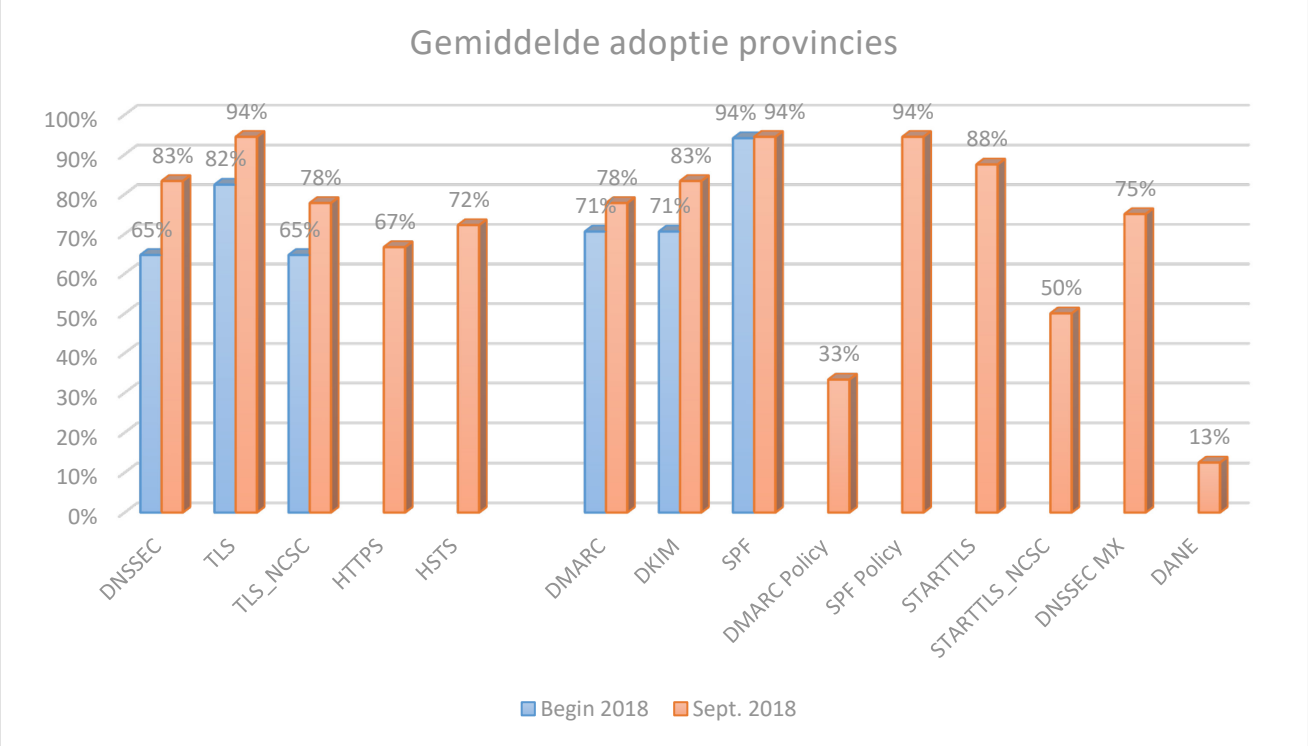
Voor de standaarden met als streefdatum uiterlijk 2019 zien we dat SPF Policy een hoge adoptiegraad heeft met 85% en STARTTLS zelfs al op 94% zit. Terwijl de gewenste configuratie (conform NCSC) nog wel wat achterblijft met 55%. Hier zie je hetzelfde als bij TLS voor web, waar de NCSC configuratie ook achterblijft, maar dat dit in de loop van de tijd wel meer naar elkaar toetrekt. De grote achterblijvers bij mail zijn DANE en DMARC Policy met respectievelijk 22% en 27% adoptie. Voor DANE is een stijging redelijk makkelijk te realiseren omdat DNSSEC MX op de 69% zit. Ook voor DMARC moet het mogelijk zijn omdat veel organisaties al wel DMARC beschikbaar hebben. Verder zien we, in lijn met de eerdere metingen, dat de aandacht voor de web-standaarden significant groter is dan de aandacht voor de mail-standaarden.

Per overheidslaag

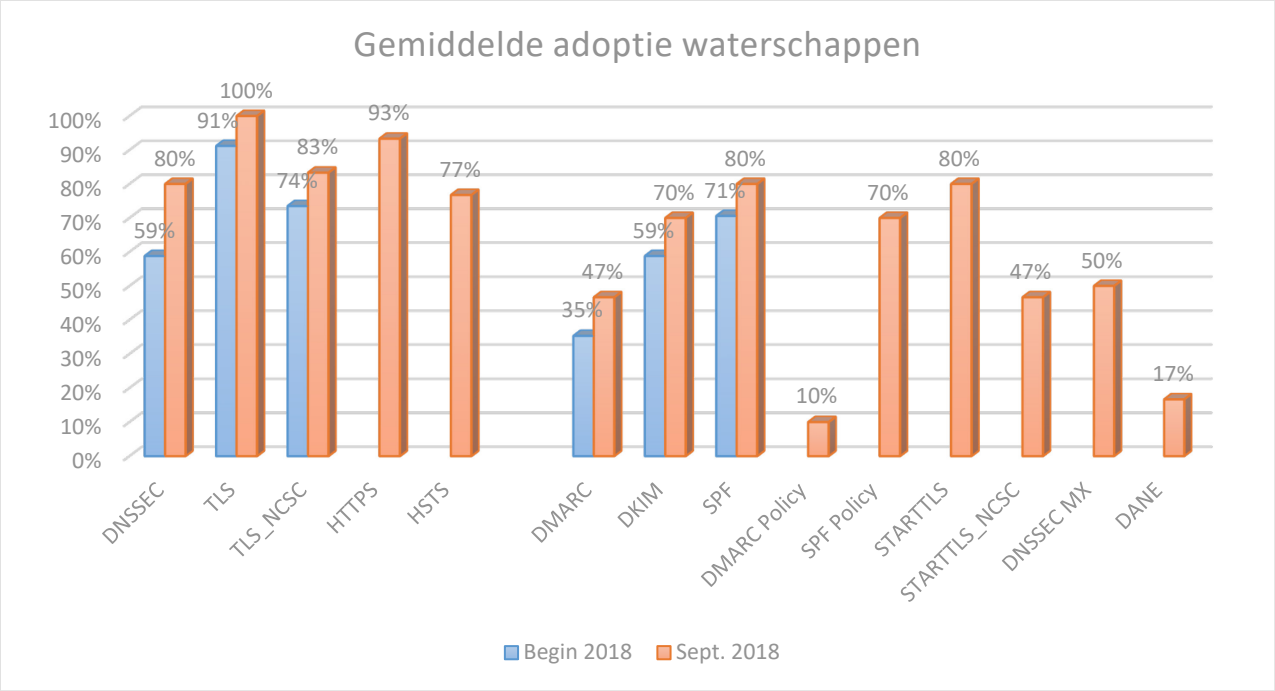
Een uitsplitsing van de resultaten naar overheidslaag laat zien dat in iedere overheidslaag de adoptie groeit. De mate van groei verschilt wel sterk, met name de waterschappen en provincies zijn sterk gegroeid met gemiddeld 12 procentpunt (waterschappen) en 10 procentpunten (provincies). Dit berekend over de standaarden DNSSEC, TLS, TLS cf NCSC, SPF, DKIM en DMARC. De waterschappen weten daarnaast 100% adoptie te realiseren voor TLS.

Wat verder opvalt in relatie tot de nieuwe streefbeeldafspraken is dat de standaard SPF Policy en de aanwezigheid van STARTTLS overal goed scoren. Terwijl voor de standaarden DANE en DMARC Policy het Rijk en de uitvoeringsorganisaties relatief beter scoren dan de provincies, waterschappen en gemeenten

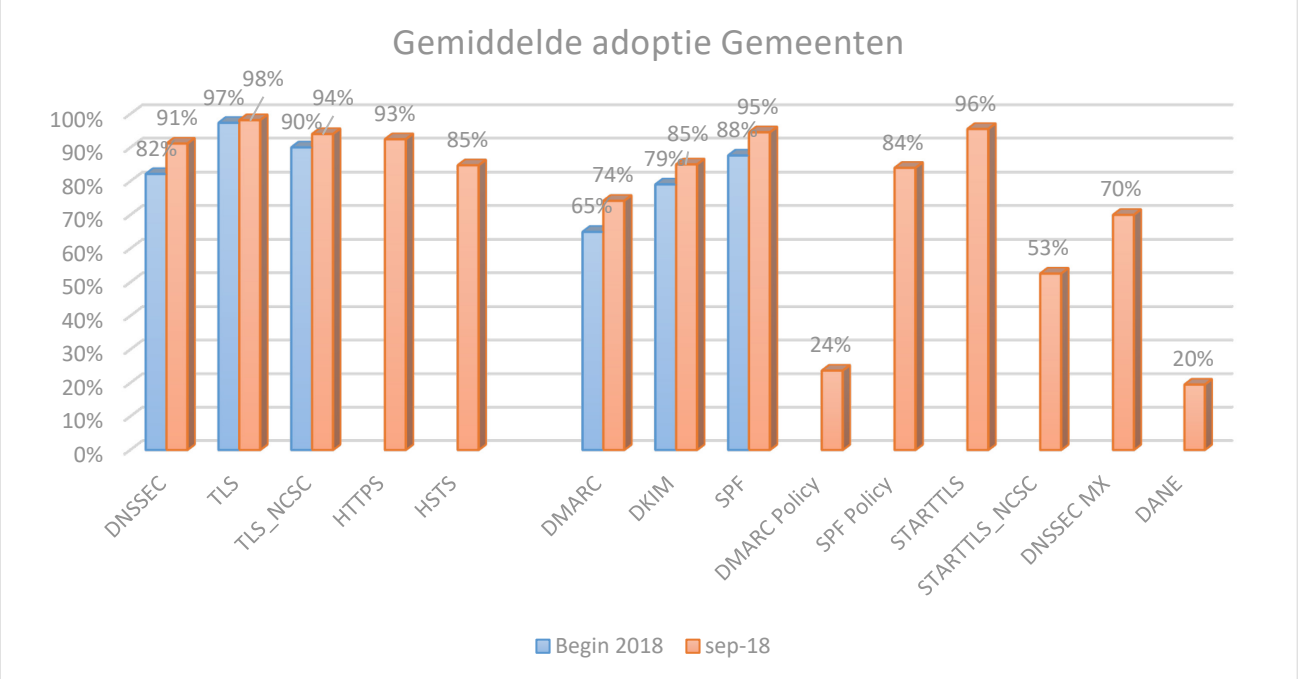
Provincies



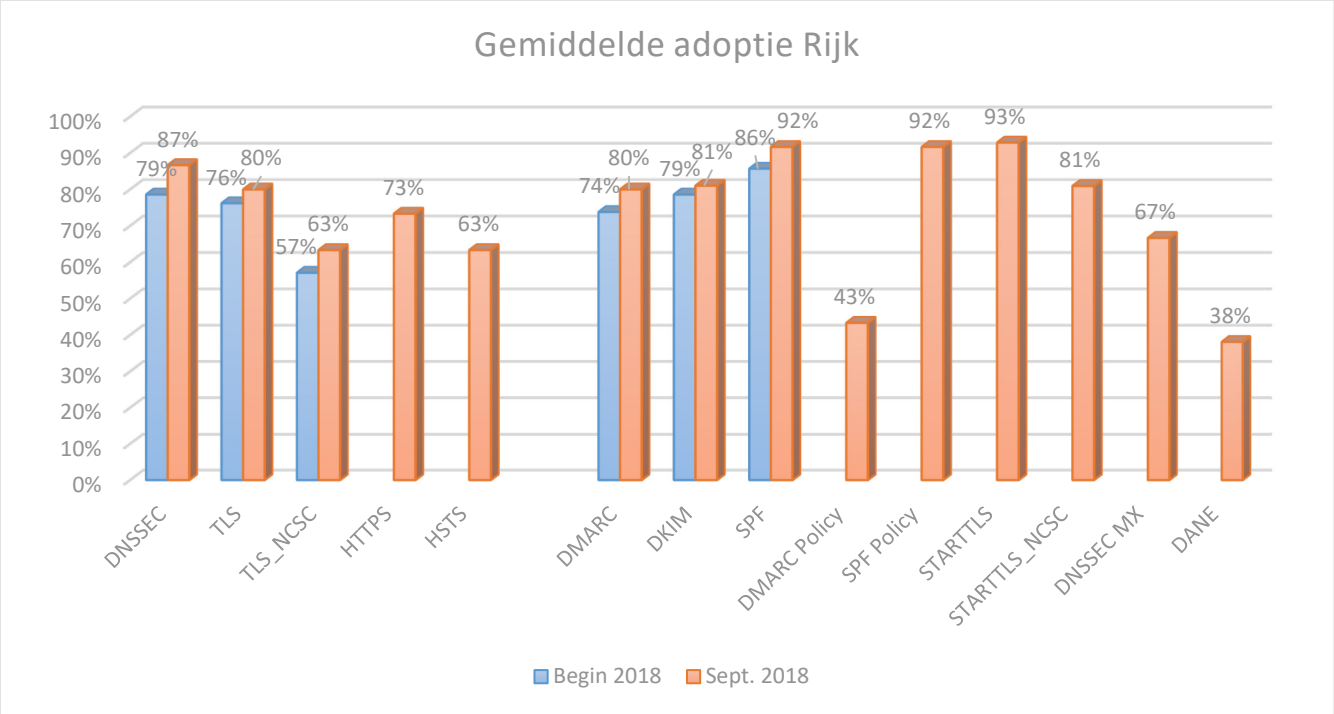
Waterschappen



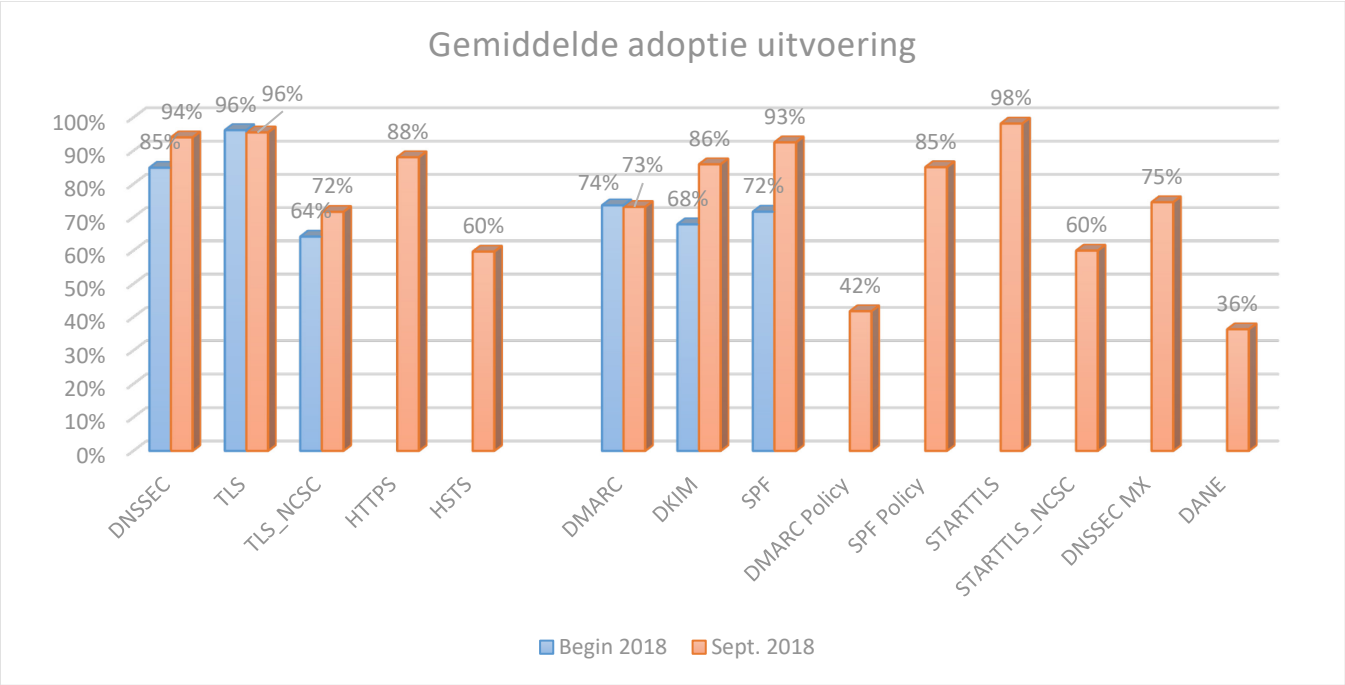
Gemeenten



Het Rijk

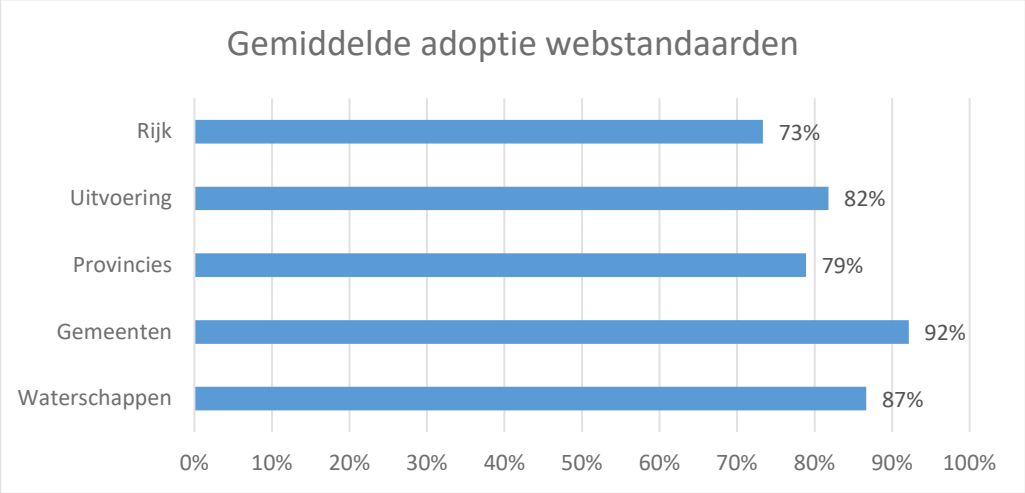


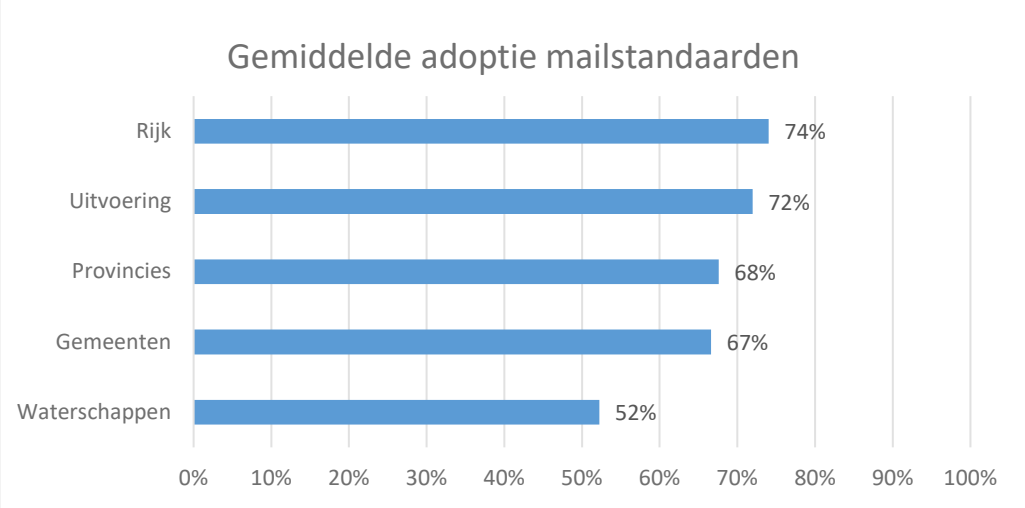
Uitvoering



Als we een vergelijking maken tussen overheidslagen voor de webstandaarden en de mailstandaarden. Dan valt op dat bij de webstandaarden de gemeenten het best scoren met een gemiddelde adoptie van 92%. Bij de mailstandaarden scoort het Rijk het hoogst met een gemiddelde adoptie van 74% en dat terwijl het Rijk juist minder scoort bij de webstandaarden. Dit laatst komt met name omdat er relatief veel

'redirect' domeinnamen van de afzonderlijke ministeries zijn getoetst in de meting. Ook deze redirects moeten goed worden dichtgezet, dit verdient daarom ook extra aandacht bij aanvullende adoptieacties. Bij de waterschappen valt op dat ze goed scoren op de webstandaarden, maar juist bij de mailstandaarden achterblijven. Voor de waterschappen is het gewenst om extra adoptieacties voor met name de mailstandaarden te organiseren.





Conclusie verklaring van de resultaten

Voor de standaarden uit de eerdere metingen (DNSSEC, TLS en TLS cf NCSC, DKIM, DMARC en SPF) zien we dat de groei doorzet, met DNSSEC als uitschieter met 10 procentpunten naar 90%. Wel valt op dat de adoptie van TLS niet tot nauwelijks meer stijgt. Om 100% te bereiken is dan ook een meer 'één op één' benadering nodig. Van de standaarden met als streefdatum uiterlijk 2018 (HTTPS, HSTS en TLS cf NCSC) zien we dat er al een hoge adoptiegraad is. Volledige adoptie voor 2019 zal echter niet worden gerealiseerd.

Als we kijken naar de nieuwe streefbeeldafspraak dan verloopt de adoptie van de standaarden SPF Policy en STARTTLS erg goed. Voor deze standaarden kan worden verwacht dat ze eind 2019 zo goed als volledig zijn geadopteerd, wel heeft de correcte implementatie van STARTTLS cf NCSC nog extra aandacht nodig. Tot slot blijft de adoptie van DMARC Policy en DANE erg achter al verschilt dit sterk per overheidslaag.

Zonder aanvullende campagnes, activiteiten en of verplichtingen zal zo goed als volledige adoptie eind 2019 lastig te realiseren zijn voor de mailstandaarden. Dit geldt in minder mate ook voor de mail-standaarden uit de eerste streefbeeldafspraak. Belangrijk is om per doelgroep te kijken welke standaarden extra aandacht nodig hebben en of er 'quick wins' zijn. Om voor de webstandaarden toch 100% te halen, is het misschien mogelijk om organisaties individueel aan te spreken en te helpen. Daarnaast kan een wettelijke verplichting helpen om de laatste paar procent zo ver te krijgen dat ze de standaarden ondersteunen.