notitie

Forum Standaardisatie
www.forumstandaardisatie.nl
forumstandaardisatie@logius.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 verplicht

FORUM STANDAARDISATIE 14 maart 2018

Agendapunt 4. Open standaarden, adoptie
Stuknummer 4a: Evaluatie en vervolg streefbeeldafspraak IV-standaarden

Samenvatting
In februari 2016 heeft het Nationaal Beraad een streefbeeld-afspraak gemaakt over de adoptie van vijf internetveiligheidstandaarden door alle Nederlandse overheden voor eind 2017. Het Forum Standaardisatie heeft elk half jaar de voortgang van deze afspraak gemonitord. Nu de betreffende periode is geëindigd kan geconcludeerd worden dat de streefbeeld-afspraak heeft geleid tot een sterke adoptie-impuls: de adoptiegraad is sinds het maken van deze afspraak ongeveer verdubbeld.

A) In het licht van dit succes wordt het Forum Standaardisatie gevraagd de opvolger van het Nationaal Beraad te adviseren om voor meer standaarden een streefbeeld-afspraak te maken.

B) Niettemin is ondanks de grote groei in de adoptiegraad het streefbeeld (volledige adoptie van de vijf standaarden) niet gehaald. Om deze reden wordt het Forum Standaardisatie ook gevraagd de opvolger van het Nationaal Beraad te adviseren om verdere actie te ondernemen om achterblijvende organisaties alsnog tot adoptie te bewegen.

Gevraagd besluit
Aan het Forum wordt gevraagd om in te stemmen met het advies om aan het OBDO de volgende punten voor te leggen:

A. Een aanvullende afspraak te maken voor eind 2019 over:
   a. de adoptie van standaarden die het mogelijk maken een beveiligde verbinding op te zetten waardoor het moeilijker wordt voor derden om mee te lezen in e-mail-verkeer.
   b. het zodanig configureren van e-mailstandaarden dat e-mail waarvan de afzender zich onterecht presenteert als representant van een overheidsorganisatie niet alleen geïdentificeerd kan worden, maar dat deze e-mails ook niet afgeleverd worden in de inbox van de ontvanger.

B. Achterblijvende organisaties via de koepels of de staatsecretaris van Binnenlandse Zaken en Koninkrijksrelaties op individuele basis aan te schrijven om de bestaande afspraak en hun achterblijvende resultaat op bestuurlijk niveau onder de aandacht te brengen.

C. Nader onderzoek te laten doen naar het gebruik van één domeinnaam-extensie naar model van het Britste gov.uk of het Duitse Bund.de.

Dit advies is gebaseerd op de resultaten die geboekt zijn door de overheid naar aanleiding van de streefbeeld-afspraak van het Nationaal Beraad om voor eind 2017 vijf internetveiligheidstandaarden (IV-standaarden) overheidsbreed geïmplementeerd te hebben. Deze resultaten worden in het vervolg van deze notitie gepresenteerd en toegelicht.

Achtergrond

Medio 2015 heeft het Forum Standaardisatie voor het eerst een meting van de adoptiegraad van vijf internetveiligheidstandaarden voor overheidsdomeinen (web en mail) uitgevoerd: de zogenoemde IV-meting.[1] De gemiddelde adoptiegraad was ten tijde van deze meting 35%. Het Nationaal Beraad hechtte een dusdanig belang aan de adoptie van deze standaarden dat het op basis van de eerste meting van het Forum 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' werd gevolgd (d.w.z. wachten op een volgend investeringsmoment en dan de standaarden implementeren). In plaats daarvan werd actief werd ingezet op volledige implementatie van de standaarden voor eind 2017. Met het maken van deze streefbeeld-afspraken wilde het Nationaal Beraad de adoptie van al deze standaarden een flinke stimulans te geven.

Onderdeel van deze afspraak was dat het Forum de voortgang van de adoptie meet en inzichtelijk maakt. Mede om deze reden meet het Forum halfjaarlijks de adoptiegraad en rapporteert het over de uitkomsten. Elke meting worden bij benadering 550 overheidsdomeinen getest[3], bestaande uit:

- Domeinen die horen bij de deelnemers van het Nationaal Beraad
- De domeinen die horen bij voorzieningen van de Generieke Digitale Infrastructuur.
- Een selectie van de best bezochte domeinen van Rijksoverheden (en uitvoerders)
- De domeinen van de andere partijen die direct of indirect vertegenwoordigd waren in het nationaal beraad, zoals:
    - Uitvoerders (de Manifestpartijen)
    - Gemeenten
    - Provincies en Waterschappen
    - Partijen behorend tot Klein LEF

Het Nationaal Beraad heeft de bovengenoemde streefbeeldafspraak gemaakt met betrekking tot de volgende standaarden:

- DNSSEC: Domeinnaambeveiliging
- TLS voor transactie-websites[4]: Beveiligde verbinding

[1] Voor deze meting wordt gebruik gemaakt van de test-instrumenten van internet.nl. Internet.nl is een initiatief van het Platform Internetstandaarden.. Vanuit de Nederlandse overheid zijn naast het Forum Standaardisatie ook NCSC en het Ministerie van Economische Zaken deelnemers aan dit Platform.

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

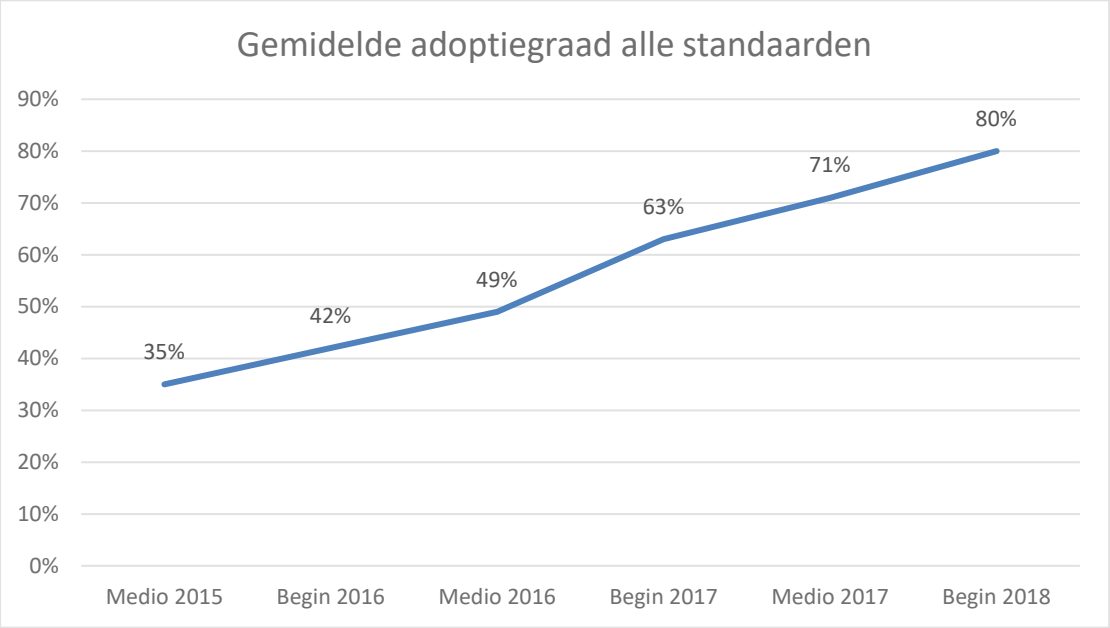
[3] De domeinen van de gemeenten worden getoetst sinds de meting medio 2016. De lijst geteste domeinen voor de metingen medio 2015 en begin 2016 bestond daarom uit ongeveer 150 domeinen.

4 Voor TLS geldt dat het Nationaal Beraad de ambitie uitsprak deze tenminste voor die domeinen toe te passen waar burgers en bedrijven mogelijk privacy -gevoelige gegevens invoeren (een zogenaamde transactiesite).

- DKIM: Anti-Phishing
- SPF: Anti-Phishing
- DMARC: Anti-Phishing (rapportages)

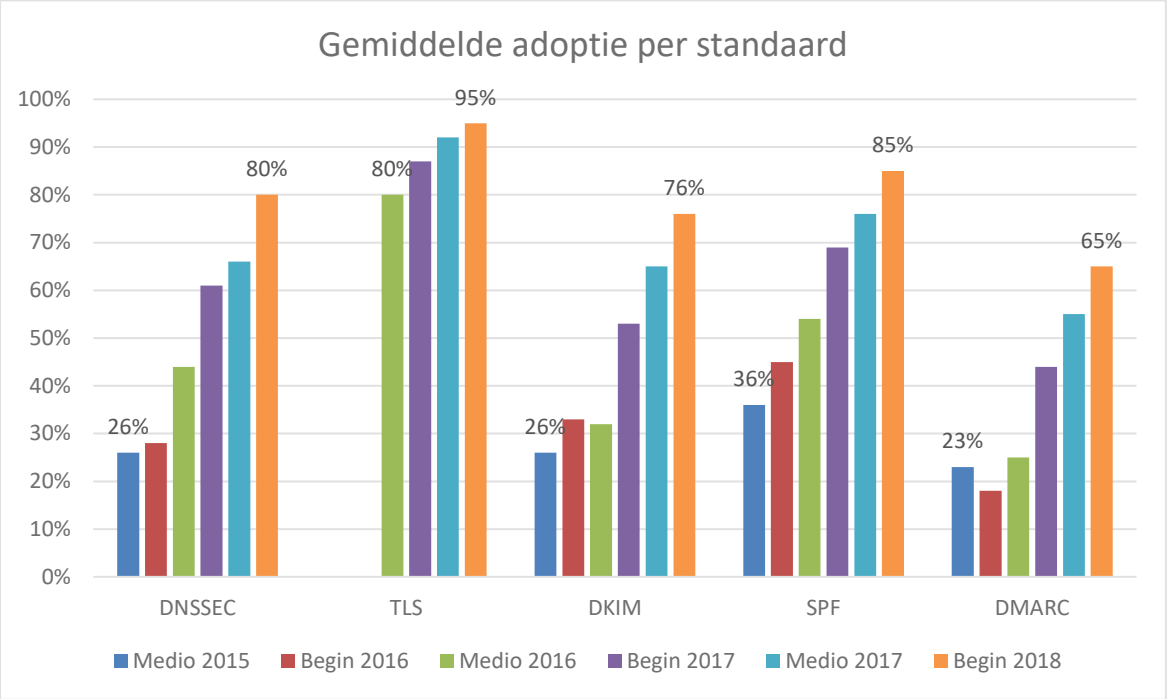
Al deze standaarden, met uitzondering van DMARC, staan op de 'pas toe of leg uit'-lijst van het Forum.[5]

Resultaten
Op 2 januari 2018 heeft het Bureau Forum Standaardisatie de IV-meting voor begin 2018 uitgevoerd. Aangezien de eerste streefbeeld-afspraak van het Nationaal Beraad afliep op 31 december 2017 kan deze meting gebruikt worden om de uitkomst van deze afspraak te evalueren. De onderstaande grafiek toont de groei van de gemiddelde adoptiegraad van alle standaarden vanaf de eerste meting medio 2015 tot de meest recente meting begin 2018.



De gemiddelde adoptiegraad in de meest recente meting is 80%. Daarmee is de gemiddelde absolute groei van alle vijf de gemeten standaarden vanaf het eerste meetmoment (medio 2015) 45 procentpunten; een ruime verdubbeling van de adoptiegraad. Deze gemiddelde absolute stijging van negen procentpunten per half jaar lijkt vooralsnog nauwelijks af te nemen. Dit is opvallend aangezien in dit soort processen relatief makkelijke verbeteringen normaliter eerst worden uitgevoerd, waardoor op de langere termijn de groei in de adoptiegraad vaak afneemt.

[5] DMARC is positief getoetst maar nog niet opgenomen op de 'pas toe of leg uit'-lijst. DMARC hangt echter dermate sterk samen met de toepassing van DKIM en SPF, dat het Nationaal Beraad besloot DMARC alvast onderdeel te maken van de 'versnelde adoptie set'.



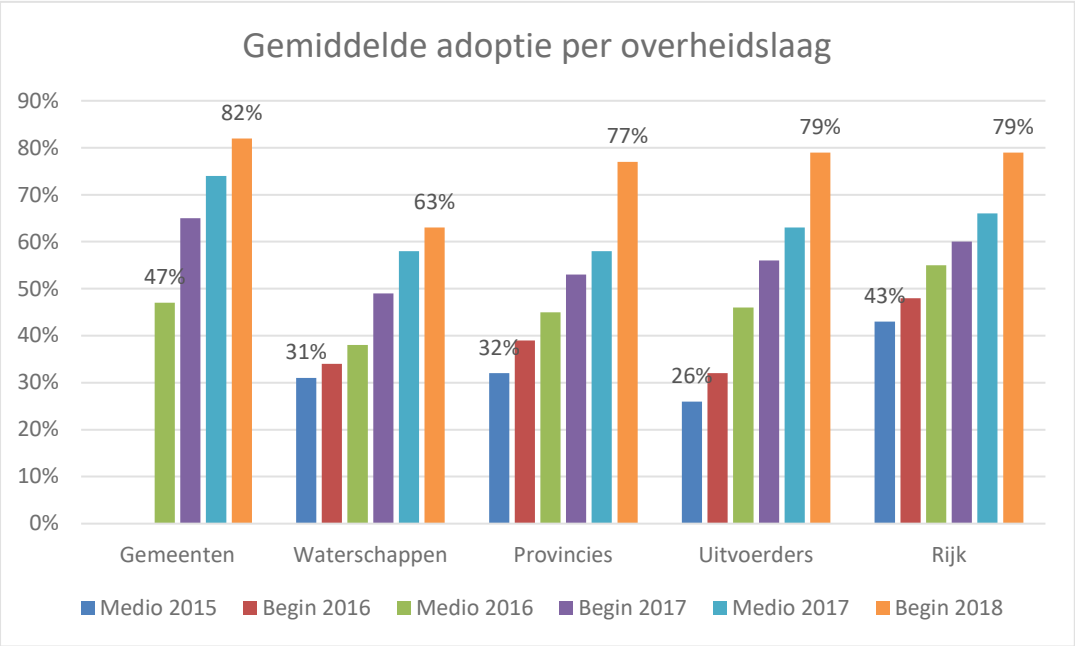
Ook als wij kijken naar de adoptiegraad van individuele standaarden (bovenstaande grafiek) zien we bij elke standaard een sterke groei.[6]

- De adoptiegraad van TLS is inmiddels bijna honderd procent. Ook bij de eerste meting was deze standaard al vrij breed geïmplementeerd. Om deze reden kent deze standaard de laagste groei in adoptie.
- De adoptiegraad van alle andere standaarden is bij benadering verdrievoudigd sinds de eerste meting.

De beveiliging van websites (middels DNSSEC en TLS) lijkt binnen de overheid grotere prioriteit te hebben dan de beveiliging van e-mail (DKIM, SPF en DMARC).

- Bijna alle geteste websites (95%) beschermen de gegevensuitwisseling met bezoekers inmiddels met behulp van TLS.
- Ook DNSSEC kent een hoge adoptiegraad (80%), en het is daarnaast de standaard die de hoogste groei vertoont.
- Aangenomen dat de groei van de afgelopen jaren aanhoudt zal gedurende 2018 vrijwel volledige adoptie van beide web-standaarden gerealiseerd worden.
- Wat betreft de e-mailstandaarden geldt hetzelfde voor SPF. De adoptie van DKIM en vooral DMARC blijven achter.

[6] *Vanwege een wijziging in de meetmethode zijn er voor de metingen medio 2015 en begin 2016 geen vergelijkbare data beschikbaar over de adoptiegraad van TLS.*



Een uitsplitsing van de resultaten naar overheidslaag (zie bovenstaande grafiek)[7] laat eveneens een sterke groei zien binnen elke categorie.

- Zowel in de pers als bij Kamervragen over informatieveiligheid wordt de aandacht vooral gericht op de adoptiegraad van IV-standaarden onder gemeenten.[8] Het is daarom opvallend dat gemeenten op dit punt gemiddeld beter scoren dan alle andere overheidslagen.
- De groei van de adoptiegraad was bij de domeinen van provincies, uitvoerders en rijk vooral sterk in het laatste half jaar van 2017. Het is aannemelijk dat dit verband houdt met het feit dat de einddatum van de streefbeeld-afspraak van het Nationaal Beraad eind 2017 lag.
- Het rijk is de enige overheidslaag waarbij de gemiddelde adoptiegraad voor alle standaarden boven de 70% ligt. Andere overheidslagen hebben moeite met het adopteren van één of meer standaarden, met name DMARC.
- Mits de huidige groei doorzet zullen alle overheidslagen, met uitzondering van de waterschappen, in 2018 vrijwel volledige adoptie realiseren voor DNSSEC, TLS, DKIM en SPF. Het is hiervoor wel van belang dat de adoptie van deze standaarden even hoog op de agenda van de betreffende overheden blijft staan als in recente jaren het geval was.
- Met de huidige groei is het niet aannemelijk dat de waterschappen binnen afzienbare termijn tot (vrijwel) volledige adoptie van de standaarden zullen komen.

Verklaring van de resultaten
Zoals hierboven beschreven is de adoptiegraad tussen medio 2015 en begin 2018 gegroeid met 45 procentpunt. Deze groei kan niet los gezien worden van de acties die mede naar aanleiding van de streefbeeld-afspraak van het Nationaal Beraad zijn ondernomen door verschillende overheden en koepelorganisaties.

- Uitgangspunt voor vrijwel al deze acties was de halfjaarlijkse meting van het Forum Standaardisatie. Deze meting wordt middels een aantal contactpersonen verspreid in alle overheidslagen. Uit de feedback op deze metingen blijkt duidelijk

[7] *Voor de domeinen van de gemeenten ontbreken gegevens voor medio 2015 en begin 2016 in de grafiek omdat deze pas vanaf medio 2016 zijn meegenomen in de meting.*
[8] *Zie bijvoorbeeld https://www.security.nl/posting/547001/Staatssecretaris%3A+Gemeenten+zijn+bezig+met+veilig+e-mailen en https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2016Z11231&did=2016D26425.*

dat overheden door deze metingen aangezet worden tot het doorvoeren van verbeteringen.

- De koepelorganisaties van de gemeenten (VNG, IBD en KING) hebben mede naar aanleiding van de streefbeeld-afspraak serieus en consistent ingezet op verbeteringen onder hun leden. Zo hebben zij hun leden regelmatig geattendeerd op de afspraken, fact sheets uitgebracht ter informatie, congressen en seminars over informatiebeveiliging georganiseerd, en de meting van het Forum Standaardisatie onder de aandacht gebracht. De grote inzet van de koepelorganisaties is voor een belangrijk deel verantwoordelijk voor de hoge adoptiegraad onder gemeenten.
- Het IPO heeft in 2017 veel gedaan om de adoptiegraad binnen provincies te verhogen. Zo is het Forum Standaardisatie in een van de provinciale overleggen uitgenodigd voor een informatiesessie en is er veel individueel contact met de verantwoordelijken binnen de provincies onderhouden.
- Ook CIO-Rijk heeft in 2017 consistent actie ondernomen om de adoptie te bevorderen. Zo worden op basis van de meting van Forum Standaardisatie de verantwoordelijken voor domeinnamen van het rijk en de uitvoeringsorganisaties aangeschreven om in kaart te brengen voor wanneer de adoptie van de standaarden gepland zijn. Indien er nog geen planning bekend is wordt er druk gezet om dit zo snel mogelijk voor elkaar te krijgen.
- NCSC heeft in de jaren sinds de gemaakte streefbeeld-afspraken een belangrijke informerende rol gespeeld ten aanzien van overheidsorganisaties, onder meer door het uitgeven van een aantal veelgebruikte fact sheets.
- Tot slot is het ook van groot belang dat de Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken, als leverancier van veel rijksoverheidsorganisaties, voor al zijn domeinnamen principieel alle standaarden implementeert die deel uitmaken van de streefbeeld-afspraak van het Nationaal Beraad.

Ondanks deze acties is het streefbeeld van het Nationaal Beraad, dat de vijf genoemde standaarden voor 2017 voor alle overheidsdomeinen geïmplementeerd moesten zijn, niet geheel gerealiseerd. Dit heeft een aantal oorzaken:

- Ondanks de grote inzet van onder meer de koepelorganisaties was eind 2017 de streefbeeld-afspraak van het Nationaal Beraad nog altijd niet bekend bij alle personen die verantwoordelijk waren voor de gemeten overheidsdomeinen.
- Er bestaat nog altijd een gebrek aan kennis over de noodzaak van standaarden binnen overheidsorganisaties. Zo wordt er regelmatig ten onrechte gedacht dat de bescherming van een domein met mail-standaarden niet noodzakelijk is als de organisatie dit domein zelf niet gebruikt voor mail.
- De implementatie van enkele standaarden is voor sommige organisaties complex. Dit geldt met name voor DMARC, hetgeen ook de relatief lage adoptiegraad van die standaard verklaart. Omdat deze standaard nog relatief nieuw is zijn er vooralsnog weinig laagdrempelige instrumenten beschikbaar voor het gebruik. Dit soort instrumenten zijn bijvoorbeeld wel beschikbaar voor TLS, en dat is terug te zien in het verschil in adoptie.
- Organisaties zijn in zekere mate afhankelijk van hun leveranciers. Dit kan positief zijn wanneer deze leverancier de standaarden zonder uitzondering implementeert, zoals de genoemde Dienst Publiek en Communicatie. Wanneer een leverancier echter een bepaalde standaard niet ondersteunt (zoals bijvoorbeeld SSC-ICT in het geval van DNSSEC), dan kan een organisatie alleen voldoen aan de afspraken door over te stappen van leverancier. Dit is niet altijd haalbaar.

Evaluatie van het Nationaal Beraad-streefbeeld
Uit het voorgaande kan geconcludeerd worden dat de streefbeeld-afspraak van het Nationaal Beraad over de adoptie van IV-standaarden voor eind 2017 een succes is geweest. Met deze afspraak werd beoogd om een grote stimulans te geven aan de adoptie van deze standaarden, en dat dit ook feitelijk terug te zien is in de resultaten. Het succes van deze afspraak is toe schrijven aan een aantal punten die meer algemeen geformuleerd kunnen worden:

- De afspraak speelt een informerende rol. Het maakt duidelijk aan organisaties wat er moet gebeuren en wanneer dit gedaan moet zijn, en dat geeft richting aan de adoptie.
- De afspraak speelt een dwingende rol. Organisaties worden aangesproken wanneer ze niet voldoen aan de gemaakte afspraak.
- De afspraak speelt een ondersteunende rol. Organisaties zoals Forum Standaardisatie die adoptie stimuleren kunnen in contact met organisaties verwijzen naar de gemaakte afspraken.

Wel dient aangemerkt te worden dat ondanks de grote groei in de adoptiegraad het streefbeeld (volledige adoptie eind 2017) niet gehaald is. Aanvullende actie is noodzakelijk om deze achterstand zo snel mogelijk weg te werken.

Advies voor continuering en aanvullende afspraken
Gezien de in de vorige sectie genoemde punten ligt het voor de hand om deze manier voor het versnellen van de adoptie van internetveiligheidstandaarden uit te breiden. Het is daarom goed dat er al een aanvullende streefbeeld-afspraak is gemaakt voor eind 2018.[9] In het Nationaal Beraad is het volgende afgesproken:

- Eind 2018 hebben alle overheidswebsites HTTPS en HSTS inclusief de veilige configuratie conform NCSC ingevoerd..
- Deze afspraak geldt voor alle overheidswebsites, en dus niet langer alleen voor zogenaamde transactiewebsites.

De voortgang van deze afspraak zal door middel van de halfjaarlijkse metingen van het Forum Standaardisatie gemonitord worden. Hierbij is het goed om op te merken dat hierdoor een wijziging in de halfjaarlijkse metingen noodzakelijk is. In eerdere metingen was het nog niet mogelijk om middels de gebruikte instrumenten voor een website te meten of HSTS geïmplementeerd was en of HTTPS werd afgedwongen. In deze metingen werd daarom alleen gekeken of TLS aanwezig was, en of deze standaard was geconfigureerd conform de aanbevelingen van NCSC. Het percentage gemeten overheidswebsites dat TLS conform NCSC-aanbevelingen heeft geadopteerd is gestegen van 26% medio 2016 naar 83% begin 2018. Vanaf de volgende meting (medio 2018) zal aanvullend hieraan gemeten worden of HTTPS wordt afgedwongen en of HSTS aanwezig is. Het percentage van de gemeten overheidswebsites dat op dit moment voldoet aan deze striktere criteria is op dit moment 61%.

De adviezen

<u>Beslissing punt A)</u>
Aanvullend zou het zinvol zijn om ook voor eind 2019 een streefbeeld-afspraak te maken voor de adoptie van een aantal aanvullende IV-standaarden en hier op te monitoren. Het Forum Standaardisatie wordt gevraagd om hierover aan de opvolger van het Nationaal Beraad, het OBDO, te adviseren. De volgende standaarden komen in aanmerking voor aanvullende afspraken:

- STARTTLS en DANE: deze standaarden voor de beveiliging van mailverkeer middels encryptie staan op de ‘pas toe of leg uit’-lijst. Het zijn geaccepteerde standaarden, waarover bijvoorbeeld ook al afspraken zijn gemaakt binnen de

[9] https://digitaleoverheid.pleio.nl/file/download/50662102

Veilige E-mail Coalitie, waarvan het Forum Standaardisatie één van de initiatiefnemers is.

- Actieve policies voor SPF en DMARC: hier wordt inmiddels ook al door verschillende overheidsorganisaties om gevraagd. Zolang er geen policy is ingesteld die de ontvanger vertelt wat te doen met verdachte e-mail biedt de aanwezigheid van SPF en DMARC op zichzelf geen extra beveiliging tegen phishing.[10]

Beslissing punt B)

Naast de genoemde voordelen kennen streefbeeld-afspraken ook één nadeel: het is mogelijk dat na de einddatum van een streefbeeld de druk op organisaties die nog niet voldoen wegvalt. Om de groei op peil te houden is het daarom essentieel dat het OBDO actie onderneemt om de achterblijvers ook in 2018 en later aan te zetten tot adoptie. Aan het Forum Standaardisatie wordt gevraagd om het OBDO te adviseren achterblijvende organisaties hetzij via de koepelorganisaties, hetzij door de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties op individuele basis aan te schrijven om de bestaande afspraak en hun achterblijvende resultaat op bestuurlijk niveau onder de aandacht te brengen.

Beslissing punt C)

Tot slot wordt het Forum Standaardisatie geadviseerd om nader onderzoek te laten doen naar de wenselijkheid en haalbaarheid om te komen tot één domeinnaam-extensie voor alle e-mailadressen van de Nederlandse (rijks)overheid. Bijvoorbeeld gov.nl of overheid.nl; voornaam.achternaam@minbzk.nl wordt dan bijv. voornaam.achternaam@bzk.gov.nl of voornaam.achternaam@bzk.overheid.nl. Omdat de in deze notitie besproken beveiligingstandaarden functioneren op domeinnaam-niveau zou een dergelijke benadering de adoptie van standaarden vergemakkelijken en overzichtelijker maken. In verschillende landen wordt deze benadering ook al toegepast: Duitsland en Engeland gebruiken respectievelijk de extensies bund.de en de gov.uk. In Nederland, daarentegen, heeft een wildgroei plaatsgevonden van overheidsdomeinen, wat aan de ene kant adoptie van standaarden bemoeilijkt, en het aan de andere kant voor ontvangers van e-mail moeilijk maakt om te bepalen of een verzender daadwerkelijk namens de overheid e-mailt.

[10] *Actieve policies zijn ~all en –all voor SPF, en p=quarantine en p=reject voor DMARC.*