20171121.09.01. Oplegnotitie agendapunt Standaardisatie

Van:	Forum Standaardisatie via Regieraad Interconnectiviteit 31-10-2017
Aan:	Nationaal Beraad 21-11-2017
Bijlagen:	A. Voorstel verlenging instellingsbesluit Forum Standaardisatie D. Planning Open Standaarden in GDI-voorzieningen

A. Ter besluitvorming - Voorstel verlenging instellingsbesluit Forum Standaardisatie
B. Ter besluitvorming - Nieuwe en aanpassingen van standaarden op de pas-toe-of-leg-uit lijst en de aanbevolen lijst
C. Ter kennisname - Outcome: spoofing volop in de media en Informatie Veiligheid standaarden
D. Ter kennisname - Planning Open Standaarden in GDI-voorzieningen (conform Digiprogramma 2017)

Ad. A. Ter besluitvorming - Voorstel verlenging instellingsbesluit Forum Standaardisatie

De huidige opdrachtgevende ministeries EZ en BZK van het Forum Standaardisatie, hebben het voornemen om het instellingsbesluit van het Forum Standaardisatie (dat eind 2017 afloopt) met vier jaar te verlengen tot en met 2021.
Zie bijlage: 20171121.09.02. Voorstel mandaatsverlenging forum standaardisatie

Graag uw akkoord met deze voorgestelde verlenging.

Ad. B. Ter besluitvorming - Pas toe of leg uit lijst en lijst aanbevolen standaarden

Zie toelichting hieronder. *Graag uw akkoord met*:

1. *Het opnemen van de STIX 1.2.1 en TAXII 1.1.1 (standaarden voor de uitwisseling van cyberdreigingsinformatie) op de 'pas toe of leg uit'-lijst en het instemmen met de aanvullende adoptieadviezen.*
2. *Het opnemen van OData 1.0 (standaard voor het gebruik van RESTful APIs) op lijst aanbevolen standaarden.*
3. *Het verwijderen van Dimensions 1.0 (een aanvullende specificatie bij de standaard XBRL 2.1 voor bedrijfsrapportages) van de 'pas toe of leg uit'-lijst en het aanpassen van het functioneel toepassingsgebied van XBRL 2.1.*
4. *Het verplaatsen van OAI-PMH 1.0 (een standaard voor de extractie van metadata) van de 'pas toe of leg uit'-lijst naar de lijst aanbevolen standaarden.*
5. *Het uniformer en eenduidiger beschrijven van de toepassingsgebieden van de Internet veiligheidstandaarden SPF, DKIM, DMARC, DNSSEC, TLS, HTTPS en HSTS.*

Toelichting op het 'pas toe of leg uit'-beleid

Het is kabinetsbeleid dat open standaarden overheidsbreed worden gebruikt op basis van een 'pas toe of leg uit'-regime voor standaarden van de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. De bekrachtiging van de standaarden die op deze lijst worden geplaatst, op advies van het Forum

Standaardisatie, ligt bij Nationaal Beraad. Daarnaast is er een lijst met aanbevolen standaarden. De standaarden op deze lijst hebben geen verplichtend karakter en zijn bedoeld als informerend en adviserend.

Overheden en semi-overheden zijn verplicht om de relevante standaarden met de status 'pas toe of leg uit' te vragen bij aanschaf of (ver)bouw van ICT -en diensten ('pas toe'). Afwijken mag alleen met zwaarwegende redenen en hierover moet verantwoording worden afgelegd in het jaarverslag ('leg uit'). Gebruik van deze standaarden verbetert de digitale communicatie (interoperabiliteit) en daarmee de samenwerking tussen overheden onderling en tussen overheden en bedrijven en overheden en burgers. Daarnaast kunnen open standaarden door iedere leverancier worden ingebouwd, wat de leveranciersafhankelijkheid (vendor lock-in) voor overheden vermindert. Het proces voor het toetsen van standaarden is transparant en robuust op basis van expertsessies en openbare consultaties.

Ad B1. STIX 1.2.1 en TAXII 1.1.1

STIX is een gestructureerde taal om cyberdreigingsinformatie te beschrijven zodat het op een consistente manier kan worden gedeeld, opgeslagen en geanalyseerd. TAXII is een transportmechanisme dat het geautomatiseerd uitwisselen van dreigingsinformatie standaardiseert. TAXII wordt gebruikt voor het uitwisselen van dreigingsinformatiedocumenten in STIX-formaat. STIX en TAXII worden beiden beheerd door OASIS.

Het NCSC heeft STIX 1.2.1 en TAXII 1.1.1 in april 2017 aangemeld voor de 'pas toe of leg uit' lijst. Een groep onafhankelijke experts heeft de twee standaarden getoetst tegen de criteria voor opname op de 'pas toe of leg uit' lijst en het expertadvies is ter openbare consultatie aangeboden.

Het Forum Standaardisatie concludeert dat STIX 1.2.1 en TAXII 1.1.1 voldoen aan de criteria voor plaatsing op de 'pas toe of leg uit'-lijst. Hierbij wordt wel aangetekend dat er behoefte bestaat aan leidraad voor eenduidig gebruik van STIX.

Meer informatie:
https://www.forumstandaardisatie.nl/sites/default/files/FS/2017/1011/FS-20171011.03A-Forumadvies-STIX-1.2.1-en-TAXII-1.1.1.pdf

Ad B2. Odata 1.0

Het Open Data-protocol (OData) is een standaard voor het gestructureerd bouwen en gebruiken van bevraagbare en interoperabele REST API's. De standaard verhoogt de gedeelde waarde van data in organisaties door de bestaande gegevenssilo's te doorbreken.

In 2016 heeft het Forum Standaardisatie een onderzoek laten doen naar REST API's. Als uitvloeisel van dit onderzoek heeft het Forum Standaardisatie OData door onafhankelijke experts laten toetsen op de criteria voor plaatsing op de lijst aanbevolen standaarden en het expertadvies is ter openbare consultatie aangeboden.

Het Forum Standaardisatie concludeert dat OData 1.0 voldoen aan de criteria voor plaatsing op de lijst aanbevolen standaarden.

Meer informatie:
https://www.forumstandaardisatie.nl/sites/default/files/FS/2017/1011/FS-20171011.03B-Forumadvies-OData.pdf

Ad B3. Dimensions 1.0 en XBRL 2.1

XBRL (eXtensible Business Reporting Language) is een standaard voor de uitwisseling van documenten en berichten waarin financiële informatie een belangrijke component vormt, zoals jaarverslagen en belastingaangiftes. XBRL wordt vaak gebruikt met aanvullende technische specificaties, waaronder Dimensions 1.0 dat samen met XBRL 2.1 op de 'pas toe of leg uit'-lijst staat vermeld.

Naar aanleiding van een onderzoek naar de adoptiestatus van XBRL en Dimensions bleek dat de verplichting van Dimensions 1.0 als aanvulling op XBRL 2.1 geen toegevoegde waarde meer heeft. Het Forum Standaardisatie heeft de verwijdering van Dimensions 1.0 laten beoordelen door onafhankelijke experts en het expertadvies is ter openbare consultatie aangeboden.

Het Forum Standaardisatie adviseert om de technische specificatie Dimensions V1.0 als aanvulling op XBRL 2.1 van de pas-toe-of-leg-uit lijst te verwijderen.

Meer informatie:
https://www.forumstandaardisatie.nl/sites/default/files/FS/2017/1011/FS-20171011.03C-Forumadvies-XBRL-v2-1-en-Dimensions-1.0.pdf

Ad B4. OAI-PMH 1.0

OAI-PMH is een standaard waarmee metadata sets uit bibliotheken met content bijeen kunnen worden gebracht om het zoeken te vergemakkelijken. Vooral de onderwijs- en erfgoedsector maken gebruik van OAI-PMH.

Een expertonderzoek in opdracht van het Forum Standaardisatie wees uit dat OAI-PMH inmiddels gangbaar is in de onderwijssector, waardoor deze standaard geen 'pas toe of leg uit'-verplichting meer behoeft ter bevordering van de adoptie. De standaard wordt ook gebruikt in de erfgoedsector, maar 'pas toe of leg uit' verplichting is daar niet aan de orde. Beide sectoren stellen op prijs dat de standaard op de lijst aanbevolen standaarden komt. Het voorstel om OAI-PMH van de 'pas toe of leg uit'lijst naar de lijst aanbevolen standaarden te verplaatsen is ter openbare consultatie aangeboden.

Het Forum Standaardisatie adviseert OAI-PMH 1.0 te verplaatsen van de 'pas toe of leg uit'-lijst naar de lijst aanbevolen standaarden.

Meer informatie:
https://www.forumstandaardisatie.nl/sites/default/files/FS/2017/1011/FS-20171011.03D-Forum advies-OAI-PMH-1.0.pdf

Ad B5. Toepassingsgebieden Internet veiligheidsstandaarden

SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC zijn standaarden voor de beveiliging van internetverbindingen, websites en e-mail. De standaarden worden genoemd in de memorie van toelichting bij de Wet GDI en in het Nationaal Beraad van 2 februari 2016 zijn aanvullende resultaatafspraken gemaakt over de adoptie van de standaarden.

Het Forum Standaardisatie startte eerder dit jaar een initiatief om de toepassingsgebieden van alle standaarden op de 'pas toe of leg uit'-lijst op een uniformere en eenduidiger manier te gaan beschrijven. Hiervoor heeft het Forum een standaardsyntaxis vastgelegd.

Een groep onafhankelijke experts heeft de functioneel toepassingsgebieden van SPF, DKIM, DMARC, HTTPS en HSTS, TLS en DNSSEC herschreven volgens de standaardsyntaxis. Het expertadvies is ter openbare consultatie aangeboden.

Het Forum Standaardisatie stelt nu voor om de toepassingsgebieden van de standaarden SPF, DKIM, DMARC, DNSSEC, TLS, HTTPS en HSTS te beschrijven volgens de standaardsyntaxis.

Meer informatie:
https://www.forumstandaardisatie.nl/sites/default/files/FS/2017/1011/FS-20171011.03E-Forumadvies-toepassingsgebieden-IV-standaarden.pdf

Ad. C. TKN - Mediaberichtgeving spoofing door gebrek aan invoering open standaarden

Ter kennisname
Zeer recent berichtten de media (o.a. het RTL- en NOS-journaal) uitgebreid over de mogelijkheid om nep-emails te versturen namens o.a. m.rutte@tweedekamer.nl en rob.bertholee@aivd.nl [1,2,3]. Dat heet *spoofing*. Hackers doen zich voor als overheidsorganisaties of personen om zo geld of inloggegevens afhandig te maken (*phishing*).
De desbetreffende overheidsorganisaties hadden toen nog geen tegenmaatregelen genomen in de vorm van de open standaarden DMARC, DKIM en SPF waarover het Nationaal Beraad vorig jaar een overheidsbrede streefbeeld-afspraak maakte.

Dit is een voorbeeld van ***outcome***, waarnaar het Nationaal Beraad vroeg bij de behandeling van de Monitor Open Standaarden 2016 ('meer duiding: wat betekenen de cijfers/wat is de maatschappelijke relevantie ervan?').

Afspraak en metingen
Het Nationaal Beraad heeft in februari 2016 in aanvulling op de 'pas toe of leg uit'-status afgesproken dat alle overheden de genoemde drie 'anti-spoofing'-standaarden voor eind 2017 implementeren.[4] Op verzoek van het Nationaal Beraad monitort het Forum Standaardisatie de voortgang van de implementatie. De laatste meting is medio 2017 uitgevoerd en is in het Nationaal Beraad van september 2017 aan de orde geweest.[5] Die liet zien dat er in twee jaar tijd een flinke adoptiegroei is bereikt, maar dat nog lang niet iedere overheidsorganisatie de afgesproken standaarden toepast. De toepassingsgraad op de gemeten 544 overheidsdomeinnamen voor DMARC, DKIM en SPF was respectievelijk 55%, 65% en 76%.

Werking 'anti-spoofing' standaarden
Met de open standaarden DMARC, DKIM en SPF kan een verzender echtheidswaarmerken toevoegen aan e-mails. De ontvanger of zijn internetprovider kan deze echtheidswaarmerken controleren en daarmee nep-mails scheiden van echte, legitieme e-mails. Het is dus van belang dat iedere overheidsorganisatie als verzender maar ook als ontvanger de genoemde open standaarden ondersteunt. Overigens dienen de standaarden ook toegepast te worden op domeinen waar niet vanaf wordt gemaild. Daarmee wordt voorkomen dat hackers vanaf die adressen phishen (burgers en bedrijven weten immers vaak niet dat er niet gemaild wordt vanaf die adressen).

Oproep en vervolg
De recente berichtgeving in de media en ook de laatste meting door Forum Standaardisatie maken duidelijk dat de overheid er nog niet is met de implementatie van de genoemde open standaarden die spoofing tegengaan. Het Forum Standaardisatie roept iedere overheidsorganisatie nogmaals op om de afgesproken standaarden te implementeren. Overheden kunnen ter ondersteuning onder meer gebruikmaken van de factsheet "Bescherm domeinnamen tegen phishing" van NCSC en de testtool Internet.nl. Ook is het Bureau Forum Standaardisatie bereikbaar voor vragen over de implementatie (info@forumstandaardisatie.nl).
Begin 2018 zal Forum Standaardisatie opnieuw een meting uitvoeren en daarover rapporteren aan (de opvolger van) het Nationaal Beraad. Bij de meting zal het Forum Standaardisatie een evaluatie van de gemaakte implementatie-afspraak voegen. Ook zal Forum Standaardisatie adviseren over het vervolg van de implementatie-afspraak en de metingen.

Naar een overheidsdomein-extensie?
Bij het definiëren van een vervolgaanpak wordt ook bekeken of de aanpak in de UK en Duitsland voor Nederland wenselijk en haalbaar is. Daar eindigen alle domeinnamen van de overheid op ".gov.uk" en

".bund.de" (bijv. publiccorrespondence@cabinetoffice.gov.uk en bsi@bsi.bund.de). In Nederland is er in de loop der tijd een wildgroei aan overheidsdomeinnamen ontstaan. Deze wilgroei maakt het enerzijds lastig om ervoor te zorgen dat iedere domeinnaam is beschermd met de genoemde 'anti-spoofing' standaarden (beheerbaarheid). Anderzijds is het voor burgers en bedrijven lastig om vast te stellen of een domeinnaam een officieel overheidsdomein is (herkenbaarheid).
Met een vaste domeinnaam-extensie, zijn overheidsdomeinen 1) makkelijker herkenbaar voor burgers en bedrijven dat ze met een overheid te maken hebben; en 2) kunnen de open standaarden tegen deze spoofing (DKIM, SPF, en DMARC) makkelijker worden geïmplementeerd.

[1] "Journalisten versturen nepmails uit naam van Mark Rutte naar Kamerleden", https://www.rtlnieuws.nl/technieuws/journalisten-versturen-nepmails-uit-naam-van-mark-rutte-naar-kamerleden
[2] "Iedereen kan mailen namens de AIVD dankzij 'spoofing'", https://nos.nl/artikel/2199557-iedereen-kan-mailen-namens-de-aivd-dankzij-spoofing.html
[3] "Niet meer mailen als Rutte: Tweede Kamer dicht lek in e-mail ", https://www.rtlz.nl/tech/niet-meer-mailen-als-rutte-tweede-kamer-dicht-lek-in-e-mail
[4] Naast DMARC, DKIM en SPF ging de afspraak ook over HTTPS/TLS (beveiligde websiteverbinding) en DNSSEC (domeinnaambeveiliging).
[5] "Halfjaarlijkse meting Informatieveiligheidsstandaarden Forum Standaardisatie, medio 2017", https://www.forumstandaardisatie.nl/sites/default/files/NB/2017/0926/NB-20170926.08.02-Halfjaarlijkse-meting-Informatieveiligheidsstandaarden-Fo....pdf

Ad. D. TKN - Planning Open Standaarden in GDI-voorzieningen (conform Digiprogramma)

Ter kennisname
In het Digiprogramma 2017 is afgesproken in 2017 een adoptieplanning op te stellen voor de adoptie van de open standaarden van de pas-toe-of-leg-uit lijst in GDI-voorzieningen.

De huidige stand van zaken is in kaart gebracht voor de Monitor Open Standaarden 2017. Daaruit blijkt dat voorzieningen voor het overgrote deel de relevante standaarden hebben ingevoerd ("V" in het schema) of de invoering hebben ingepland ("G" in het schema). De GDI-voorzieningen in de bijlage zijn gerangschikt op beheerorganisatie. De beheer organisaties zijn gevraagd een *inschatting* af te geven t.a.v. de nog niet geadopteerde of ingeplande standaarden ("N" in het schema). Voor zover ontvangen is de inschatting verwerkt ("I" in het schema). Nagekomen inschattingen zullen per alsdan worden verwerkt.

20171121.09.03. Planning open standaarden in GDI-voorzieningen