Aanbiedingsformulier

Betreft
Standaardisatie (toegelicht door Forumvoorzitter Nico Westpalm van Hoorn)

Contactpersoon
Erik Jonker
erik.jonker@digicommissaris.nl

Datum
25 januari 2016

Kenmerk
2016-0000054362

Bijlagen
5

Aanleiding

In de regieraad Interconnectiviteit van 12 januari 2016 is besloten tot doorgeleiding van een viertal stukken aan het Nationaal Beraad. Het gaat om:

a. De managementsamenvatting van Monitor Open Standaarden 2015 (bijlage a);
b. 1-meting Informatieveiligheidstandaarden (bijlage b);
c. Het werkplan Forum Standaardisatie 2016-2017 (bijlage c);
d. Nieuwe standaarden op de pas-toe-of-leg-uit lijst (bijlage d).

Het Nationaal Beraad wordt om de volgende besluiten gevraagd:

- Aangaande (Managementsamenvatting van) Monitor Open Standaarden 2015 (a) en 1-meting Informatieveiligheidstandaarden (b):
U wordt geadviseerd om het tempo van de adoptie van open standaarden, en met name deze informatieveiligheid standaarden in uw organisaties/bij uw achterban te bevorderen. Het Forum kan daarbij ondersteunen.

- Aangaande het Werkplan Forum Standaardisatie 2016-2017 (c) en nieuwe standaarden op de pas-toe-of-leg-uit lijst (d):
U wordt geadviseerd met deze stukken in te stemmen.

Deze stukken en de aan het Nationaal Beraad gevraagde besluiten worden van duiding voorzien in een notitie van het Bureau Forum Standaardisatie (onderliggend aan dit aanbiedingsformulier).

Van: Forum Standaardisatie via de regieraad Interconnectiviteit
Aan: Nationaal Beraad
Betreft: Notitie Standaardisatie (toegelicht door Forumvoorzitter Nico Westpalm van Hoorn)

1. Bespreken van:
   a) Managementsamenvatting Monitor Open Standaarden 20151, en de daaropliggende duiding en maatregelen (bijlage a);
   a) 1-meting InformatieVeiligheid-standaarden (bijlage b)

   Implementatie van Open Standaarden gaat nog onvoldoende snel. Het Forum kan ondersteunen, maar voor implementatie staan overheidspartijen zélf aan de lat. Omdat informatieveiligheidstandaarden van groot belang zijn voor de veiligheid van de GDI en de daarop gebaseerde dienstverlening, rapporteert het Forum om het half jaar over de stand van zaken.
   U wordt geadviseerd om het tempo van de adoptie van open standaarden, en met name deze informatieveiligheid standaarden in uw organisaties/bij uw achterban te bevorderen. Het Forum kan daarbij ondersteunen.
2. Instemmen met werkplan Forum Standaardisatie 2016-2017 (bijlage c)
3. Instemmen met opnemen van drie standaarden op de 'pas toe of leg uit'- lijst (bijlage d)

Ad. 1 Ter bespreking Monitor 2015 + 1-meting Informatieveiligheid standaarden

Monitor 2015
Jaarlijks wordt in opdracht van het Forum Standaardisatie een monitor-onderzoek gedaan naar de stand van zaken rond open standaarden. In deze monitor wordt gemeten: 1) naleving Rijksinstructie Open Standaarden en overheidsbrede pas-toe-of-leg-uit afspraak[2]; 2) het gebruik van standaarden in voorzieningen (o.a. GDI-voorzieningen); en 3) gebruiksgegevens van standaarden.
Bovenop de management samenvatting van de monitor treft u een duiding van de monitor door het Forum standaardisatie, de maatregelen die door het Forum genomen worden naar aanleiding van de monitor, en voor een snel overzicht een tweetal *infographics* over de voortgang,

1-meting Informatieveiligheidstandaarden
Daarnaast is in het Nationaal Beraad van 18 mei jl. afgesproken dat de leden van het Nationaal Beraad het gebruik van Informatieveiligheid standaarden[3] in hun organisaties actief stimuleren, en dat de Digicommissaris hen erop zal aanspreken wanneer de adoptie onvoldoende snel gaat. Daarom is in de zomer van 2015 een 0-meting van het daadwerkelijk gebruik van deze standaarden bij domeinnamen van de partijen in het Nationaal Beraad[4] gedaan (met behulp van internet.nl), en is eind 2015 een 1-meting uitgevoerd.

Waarom een extra focus op veiligheid standaarden (naast pas-toe-of-leg-uit in aanbestedingen)?
- Burgers en bedrijven mogen van de overheid verwachten dat elke vorm van datatransport over publieke netwerken adequaat wordt beveiligd. Dit is een voorwaarde om de doelstelling van Digitaal 2017 te verwezenlijken.
- Burgers en bedrijven moeten op de echtheid van een overheidssite of e-mail kunnen vertrouwen. Dat kan slechts indien genoemde standaards zijn geïmplementeerd, daarover bestaat brede consensus bij overheid, wetenschap en bedrijfsleven. Het belang van deze standaarden wordt overheidsbreed erkend.

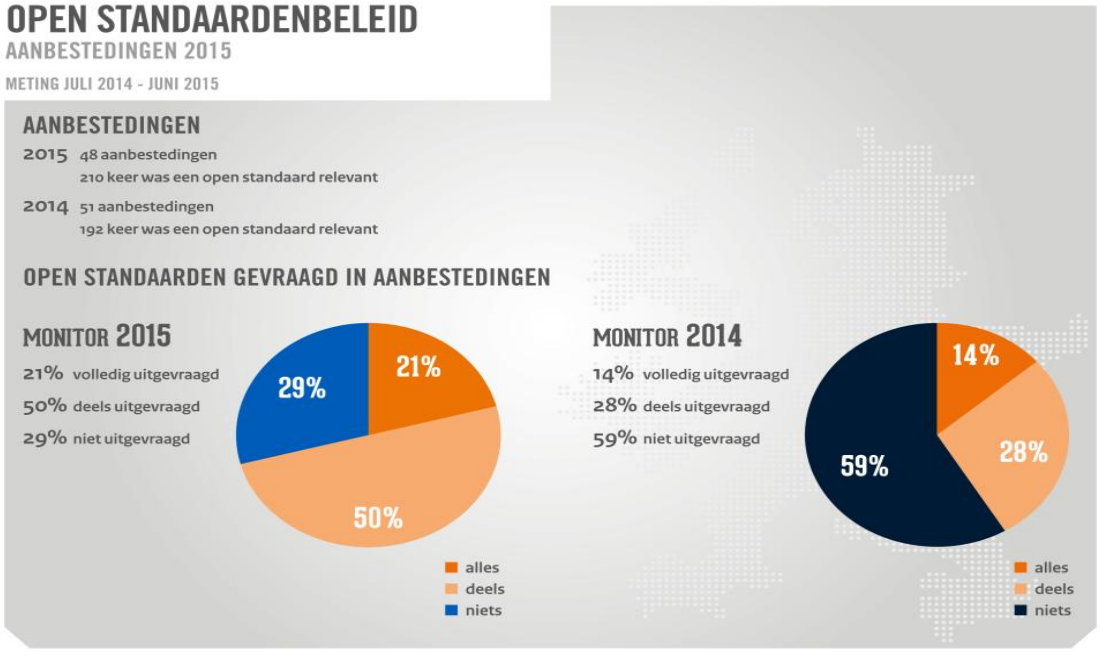
[1] Het gehele rapport is hier te vinden: https://www.forumstandaardisatie.nl/sites/default/files/NB/2016/0202/Monitor-OSb-2015-Definitief-PDFversie.pdf
[2] Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten (Staatscourant 2008, nr. 227), waarvan is afgesproken die overheidsbreed toe te passen.
[3] Het betreft het gebruik van het goede slotje op overheids-websites (TLS) en DNSSEC (beide anti-website fraude) en het gebruik van DKIM, SPF, DMARC (anti-email fraude).
[4] Het betreft de partijen in het Nationaal Beraad zelf, en de partijen daar vlak tegenaan. Ten aanzien van gemeenten zullen de resultaten van de impact-analyse van VNG/KING worden afgewacht.

- Elke ICT-voorziening die gebruik maakt van publieke netwerken/ het Internet zal voortdurend bloot staan aan actuele dreigingen en ook de beheers- en onderhoudssituatie dient daarop zo snel mogelijk te worden ingericht met effectieve beveiligingsniveaus.
- Kosten van implementatie zijn te overzien: het gaat enerzijds om honderden euro's per jaar (anti-website fraude: TLS & DNSSEC) en anderzijds om duizenden euro's (anti e-mail fraude: DKIM & SPF)[5]
- De voortgang van het gebruik van deze standaarden kan geautomatiseerd centraal worden gemeten (2 keer per jaar), daarvoor hoeven de organisaties zelf niet te worden lastig gevallen.

Resultaten

a. Monitor Open Standaarden

De monitor (zie bijlage a, en figuur 1) laat een flinke verbetering ten opzichte van voorgaande jaren zien, maar ook dat de overheid nog niet op motie-niveau[6] is (de door de regering overgenomen motie vraagt erom dat eind 2015 *alle* overheidsaanbestedingen aan pas-toe-of-leg-uit voldoen).



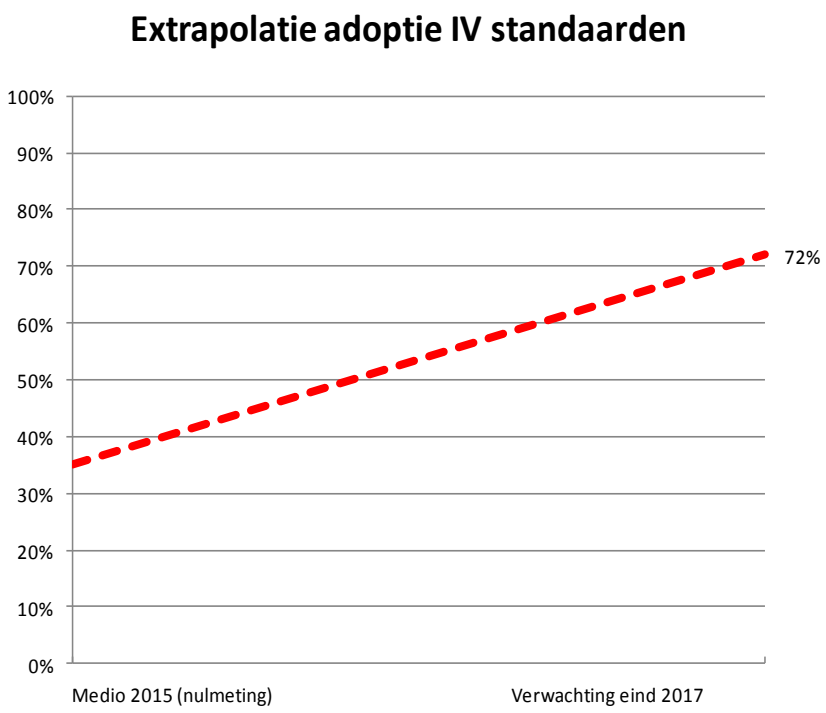
Figuur 1: aanbestedingen in de monitor 2015 vergeleken met 2014

b. 1-meting **i**nformatie**v**eiligheid standaarden (IV standaarden)

Extrapolatie van de gemeten halfjaars-groei van het gebruik van de informatieveiligheid standaarden geeft een beeld waar de overheid eind 2017 staat (zie figuur 2).

[5] Indicatie ordegrote kosten incl. bandbreedte: anti-website fraude: eenmalig 400€, 700€ per jaar (TLS + DNSSEC); anti-email fraude: eenmalig 2.500 € tot 10.000€, jaarlijks 1.250 € tot EUR 5.000 € (DKIM, SPF, DMARC).

[6] Motie Oosenbrug/Gesthuizen, Tweede Kamer, vergaderjaar 2014–2015, 33 326, nr. 21 2



Figuur 2: extrapolatie groei naar eind 2017[7]

Dat is problematisch omdat eind 2017 *alle* overheidsdienstverlening digitaal mogelijk moet zijn. Het niet op orde hebben van de informatieveiligheid bij de resterende domeinnamen leidt tot veiligheidsrisico's door website- en e-mail fraude. Daarnaast is het niet goed uit te leggen dat nu meer dan de helft, en in 2017 een kwart van de overheid onveilig digitaal communiceert.

U wordt gevraagd aan de hand van bovenstaande punten te bespreken hoe de adoptie van open standaarden van de pas-toe-of-leg-uit lijst in het algemeen (motie Oosenbrug/Gesthuizen), en deze informatieveiligheid standaarden in het bijzonder, in overheidsorganisaties en ook in uw organisaties verder kan worden gebracht.
Het Forum Standaardisatie ondersteunt graag bij de implementatie (zie laagdrempelige steun onder de adoptie maatregelen, bijlage a, p. 2).

Ad. 2 Werkplan Forum Standaardisatie 2016-2017
Volgens het instellingsbesluit van het Forum Standaardisatie dient het Nationaal Beraad het Forum werkplan goed te keuren.

Ook voor de periode 2016 en 2017 zet het Forum in op de adoptie van standaarden. Daar is ook reden voor, zie het rapport van de commissie Elias (aanbeveling 9: 'handhaaf open standaarden beleid'), de Motie Oosenbrug/Gesthuizen ('voor eind 2015 alle aanbestedingen conform pas-toe-of-leg-uit'), en de Monitor Open Standaarden 2015 ('flinke verbetering ten opzichte van voorgaande jaren, maar we zijn nog niet op motie-niveau').

Ad. 3 Instemmen met het opnemen van een drietal standaarden
Instemmen met de opname op de 'pas toe of leg uit'-lijst van:

a) Een standaard voor wifi netwerken (WPA2-Enterprise);
b) Een standaard voor archeologische informatie (SIKB0102), en het toekennen van 'uitstekend beheer' status;
c) Een nieuwe versie van een standaard voor juridische informatie (BWB) , en het toekennen van uitstekend beheer.

[7] Een uitgebreider overzicht van de extrapolatie per standaard vindt u in bijlage b.