Follow-up stemming-peilen adoptie-impuls

Vergadering:	Forum Standaardisatie 19 juni 2024
Agendapunt:	5A
Documentnummer:	FS-20240619.5A
Aan:	Forum Standaardisatie
Van:	Bureau Forum Standaardisatie
Bijlagen:	NVT
Rechten:	CC0 publieke domeinverklaring

Voorstellen

A. Voorstel is om een brief over toezicht en handhaving aan BZK te schrijven, in afschrift aan het OBDO. Daar waar mogelijk, kan het bureau helpen met de voorbereiding, bijvoorbeeld door de reeds bestaande toezichtsmogelijkheden op grond van de wet te beschrijven (die betreffen met name de rijksoverheid).

B. Voorstel is dat Forumleden van wie de eigen koepel en/of achterbannen vallen onder het ‘pas toe of leg uit’ beleid en/of de wettelijke verplichting (zie achteraan de notitie) met het hoger management in eigen koepel in gesprek gaan over adoptie en daarbij proberen hun CIO’s aan de slag te krijgen voor adoptie. Daarnaast geven zij een presentatie in hun achterban of koepel, desgewenst ondersteunt door het bureau. Het bureau zal de stand van zaken bijhouden in het bestaande reguliere overzicht met activiteiten per lid.

Aan de leden van het Forum wordt gevraagd of zij met beide voorstellen akkoord kunnen gaan.

Toelichting

In de Forum-vergadering van 28 februari is de stemming gepeild ten aanzien van verschillende mogelijke acties om de achterstand in de adoptie van informatieveiligheidstandaarden bij de groep achterblijvers (25 a 45%), in te lopen.

Forumleden konden op een schaal van 1 tot 5 aangeven, welke acties verder zouden kunnen worden uitgewerkt, en (indien nodig) voor besluitvorming terug konden komen, en of doorgeleid naar het OBDO. Deze notitie bevat de acties die 3.5 punten of hoger scoorden, op een schaal van 5. Dat gold voor 14 van de 20 acties.
Daarnaast bevat de notitie een aantal suggesties uit het Forum.

Goed scorende acties

Drempel 3.5 (schaal van 1 tot 5) of hoger

1. Op DG niveau praten met Audit Dienst over naleving afspraken en handhaving 'pas toe of leg uit' rijksinstructie en rijksbegrotingsvoorschriften (score 3.8)

2. Brief Staatssecretaris aan achterblijvers wettelijk verplichte standaarden (score 3.6)

7. Toezicht op wettelijk verplichte (WDO art.3) standaarden moet worden geregeld in een wet (score 3.9)

8. Huidige WDO biedt al diverse toezichtmogelijkheden. Die gaan we benutten (score 3.9)

9. Huidige 'Pas toe of leg uit' rijksinstructie moet overheidsbreed, en daarom wettelijk geregeld (3.9)

10. Instellen van een verplichte toets op standaarden vooraf, bij projectvoorstellen / aanbestedingen (score 4.3)

11. Verweven van de 'pas toe of leg uit standaarden': Informatie Veiligheid standaarden (IV-standaarden) moeten in NIS2 (score 4.1)

12. Forumleden gaan met hoger management in eigen koepel in gesprek over adoptie (score 3.9)

13. Forumleden geven zelf presentatie in hun koepel over adoptie (score 4.2)

14. ('overheids') Forumleden proberen hun CIO's aan de slag te krijgen voor adoptie (score 4.0)

15. IV-meting bevat alleen hoofddomeinen van gemeenten, provincies, waterschappen. Net als bij rijk en uitvoering gaan we ook hun andere domeinen meten (score 4.4)

16. Het rijks-overleg over betere regie op internetdomeinen (websites & e-mail) voorheen BID verbreden naar gemeenten, provincies en waterschappen (score 3.9)

18. Vanuit Strategisch Leveranciersmanagement Rijk moet structureel gestuurd worden op de daadwerkelijk ondersteuning van open standaarden door leveranciers (score 4.9)

20. We maken een openbaar leg-uit register (score 3.8)

Stand van zaken & voorstel

Deze acties laten zich indelen in:

a) Toezicht en handhaving
b) Acties forumleden
c) Overig

Ad. a) Toezicht en handhaving

De actiehouder van de acties onder deze noemer, is het ministerie van BZK. Het gaat immers over (8) het benutten van de bestaande toezichtmogelijkheden rond verplichte standaarden op grond van artikel 3 WDO (veelal Rijks gericht). Het wettelijk regelen van overheidsbreed toezicht (7) op die wettelijk verplichte standaarden. En over het verweven van de Informatie Veiligheidstandaarden (IV-standaarden) in NIS2 (11).

Verder over het (zoals eerder in het OBDO afgesproken) op DG niveau praten met Audit Dienst over naleving afspraken en handhaving 'pas toe of leg uit' rijksinstructie en rijksbegrotingsvoorschriften (1), en over het schrijven van een brief door de Staatssecretaris aan achterblijvers van wettelijk verplichte standaarden.

Gelet op de aard van de acties (waaronder wetgeving, en de uitleg ervan), is het ministerie van BZK actiehouder. Het Forum Standaardisatie kan over dit onderwerp gevraagd of ongevraagd advies te geven.

Voorstel toezicht en handhaving

Voorstel is daarom, om een brief hierover aan BZK te schrijven, in afschrift aan het OBDO. Daar waar mogelijk, kan het bureau helpen met de voorbereiding, bijvoorbeeld door de reeds bestaande toezichtsmogelijkheden op grond van de wet te beschrijven (die betreffen met name de rijksoverheid). Het Forum zal in haar advies ook de wenselijkheid te benoemen om toezicht en handhaving in een bestaande pdca-cyclus mee te nemen, met het oog op effectiviteit, efficiëntie en behapbaarheid.

Ad. b) Acties Forumleden

Een set acties beschrijft dat Forumleden met hoger management in eigen koepel in gesprek gaan over adoptie (12), en daarbij proberen hun CIO’s aan de slag te krijgen voor adoptie

(14). Daarnaast geven zij een presentatie in hun achterban of koepel (14). Dat sluit goed aan bij de in het instellingsbesluit genoemde verwachte activiteiten van elk Forumlid (art. 3 lid e Instellingsbesluit Forum Standaardisatie 2022-2026).

Voorstel acties Forumleden

Voorstel is dat Forumleden die vallen onder het 'pas toe of leg uit' beleid en/of de wettelijke verplichting deze acties oppakken (zie achteraan deze notitie).Het bureau zal de stand van zaken bijhouden in het bestaande reguliere overzicht met activiteiten per lid. Desgewenst kan het bureau van het Forum ondersteunen bij de activiteiten.

Ad. C) Overige acties

BFS pakt zelf de volgende punten op:

15. IV-meting bevat alleen hoofddomeinen van gemeenten, provincies en waterschappen. Net als bij rijk en uitvoering gaan we ook hun andere domeinen meten (15).

16. Het rijks-overleg (BID-R) over betere regie op internetdomeinen (websites & e-mail) heeft op 4 april een succesvolle doorstart bijeenkomst gehad, en zal weer periodiek bij elkaar komen. Aan het OBDO zal worden aangeboden het overleg te verbreden naar gemeenten, provincies, uitvoeringsorganisaties, waterschappen en andere publieke instellingen (desgewenst met een specifieke bijeenkomst).

18. In adviezen van het Forum aan het OBDO, zal worden voorgesteld vanuit Strategisch Leveranciersmanagement Rijk (SLM-Rijk) structureel te sturen op daadwerkelijk ondersteuning van open standaarden door leveranciers, en op versterking van de rol van SLM. Ondermeer in het kader van Cloud, open standaarden en vendor-lockin (zoals naar voren kwam in het recente Cloud onderzoek van het Forum).

De overige drie acties die in stemming waren gebracht en hoog scoorden zijn met het oog op de beperkte capaciteit vooralsnog niet uitgewerkt:

9. Huidige 'Pas toe of leg uit' rijksinstructie moet overheidsbreed, en daarom wettelijk geregeld

10. Instellen van een verplichte toets op standaarden vooraf, bij projectvoorstellen / aanbestedingen

20. We maken een openbaar leg-uit register

Daarnaast is een aantal suggesties voor andere acties gedaan. Die gaan veelal over vorm & toon, en lenen zich minder voor een individuele reactie. We nemen de suggesties mee in onze werkzaamheden:

i. SLM rijk niet alleen laten onderhandelen met de leveranciers. Maar ook meer sturen op de uitvragende partijen dat zij verplicht zijn standaarden uit te vragen.

ii. Geef medeoverheden alleen een .overheid.nl of .gov.nl domein als zij voldoen aan de wettelijke verplichte IV standaarden voor die domeinen.

iii. Positioneer dit als uitvoering en lift mee op beweging dat politiek en beleid zich beter moeten richten op uitvoering (echte werkelijkheid vs. politieke werkelijkheid)

iv. Gebruik bestaande middelen en kanalen. Activisme werkt contraproductief

v. Kies een specifieke standaard en voer daar actie op. DKim bijvoorbeeld.

vi. Solution partner programma. daar zit implementatie in andere sectoren leert ervaring dat druk vanuit inkopende partij helpt omdat daar penalties uitgeoefend kunnen worden

vii. Onafhankelijke organisatie in het leven roep leid vaak tot discussies, niet tot oplossing

viii. Verhogen adoptiegraad is heel veel praten, wel gecoördineerd.. heeft niet altijd hoogste prio, dus separaat iemand verantwoordelijk maken helpt. KPI geven aan iemand.

ix. Conformeer je als overheid aan de markt "gangbare" standaarden, waarom ben je anders dan de markt?

x. Ga uit van de overheid, ontschot, en niet alleen Rijk

xi. geef duidelijk aan wat de oude standaard was en wat de nieuwe wordt. Het is soms onduidelijk van waar we vandaan komen.

xii. Geef meer techniek-vrije-uitleg aan bestuurders en beleidsmakers. Het duizelt mij soms op dit onderwerp.

xiii. Werk met referentie implementaties / partijen die het goede voorbeeld geven

xiv. Wettelijke verplichting voor gebruik van verplichte standaarden. Stop met “leg-uit”.

xv. Werk met voorbeelden: wet gebeurt er als je niet voldoet aan een standaard.

xvi. Naar analogie van de DigiD-audit: als een partij wettelijk verplichte standaarden niet implementeert gaan de web-site en andere applicaties "op zwart"

xvii. Bestuurders gericht informeren over kansen (wat is de "business case", wat kun je als je een standaard implementeert dat je nu niet kunt) en risico's (welk risico loop je als je de standaard niet implementeert.

xviii. De (eventuele) toezichthouder moet "tanden hebben", met andere woorden: moet sancties kunnen opleggen. Als de toezichthouder dat niet kan is hij een papieren tijger.

xix. 1. Balans vinden tussen verplichten en verleiden 2. Ondersteuning bieden in handelingsperspectief (voorlichting, begeleiding, …) 3. Bestuurders aanspreken, voorlichten, begeleiden (uiteindelijk altijd verantwoordelijk, hoezo niet duidelijk?).

xx. Adoptieteams (a la ipv6).

xxi. Aansluiten bij risicomanagement (PDCA).

xxii. Standaardiseren gaat ook (vooral) over ketens. Die zie ik in de aanpak niet terug - Standaardiseer de ambitie bestuurlijk (b.v. we geven de burger persoonlijk inzicht in datagebruik) zodat dit een opdracht is om de onderliggende standaarden te implementeren.

xxiii. Verzorg presentaties voor Rijk, gemeenten enz. Over het wel en wee van standaarden.

xxiv. Promoten van het NRI, verplicht stellen bij NIS2 compliance

xxv. Stop met dreigen, zeuren en dwingen. Ga uit van de aanname dat organisaties wel willen maar lastig kunnen, dus HELP ze.

xxvi. Knelpunten bij leveranciers identificeren, en vervolg aan geven.

xxvii. We moeten ook de architecten hierin een nadrukkelijke rol geven.

xxviii. Organiseer een soort van professionele intervisie bijeenkomsten zodat partijen van elkaar kunnen leren

xxix. Bovenliggende visies moeten worden aangehaald bij “leg uit”.

Bijlage: wie vallen onder de verplichtingen?

Onder de wettelijke verplichting om https/hsts te implementeren vallen:

Overheidsorganisaties die bestuursorgaan zijn als bedoeld in artikel 1:1, eerste lid, onderdeel a, van de Algemene wet bestuursrecht(link naar andere website). Bij deze zogeheten a-bestuursorganen gaat het om de organen van de Staat (mits niet uitgezonderd), provincies, gemeenten, waterschappen en andere rechtspersonen die krachtens publiekrecht zijn ingesteld.

Dat geldt voor organisaties in de achterban van:

- Bert Voorbraak, secretaris (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Logius)
- Guido Bayens (voorzitter Architectuurraad Digitale Overheid)
- Rudi Bekkers (Technische Universiteit Eindhoven, krachtens publiekrecht ingesteld)
- Anton Grootendorst (Provincie Utrecht, Interprovinciaal Overleg)
- Peter den Held, gemeente Rotterdam
- Marc van Hilvoorde (Ministerie van Financiën, CIO-Office)
- Floor Jas (SURF)
- Gino Laan (RINIS)
- Isabel van der Leij (Rijksinspectie Digitale Infrastructuur zélf)
- Friso Penninga (Geonovum)

- Theo Peters (VNG Realisatie)
- Olivier van der Post (CIO Rijk)
- Anke Sikkema (Ministerie van Economische Zaken en Klimaat)
- Gerard Smits (het Waterschapshuis)
- Geert-Jan van de Ven (Manifestgroep/CIP)
- Lindy van de Westelaken, (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)

Nota bene, de verplichting geldt niet persé voor alle organisaties in hun achterban:

1. Surf is zelf geen a-bestuursorgaan, maar deze specifieke verplichting is wel van toepassing op de volgende leden van SURF: Universiteit Leiden, Rijksuniversiteit Groningen, de Universiteit Utrecht, de Universiteit van Amsterdam, de Universiteit Maastricht, Erasmus Universiteit Rotterdam , Universiteit Twente, en de Landbouwuniversiteit Wageningen, Technische Universiteit Delft, en de Technische Universiteit Eindhoven.
   De overige universiteiten (VU, Radboud en Tilburg) vallen hier niet onder (want zijn opgericht krachtens privaatrecht). Datzelfde valt te zeggen voor alle hogescholen en de bij SURF aangesloten MBO scholen.