notitie

FORUM STANDAARDISATIE 9 DECEMBER 2020
Agendapunt 4C - Duiding en Maatregelen Monitor

Nummer:	FS-20201209.4C1 **CONCEPT**
Aan:	Forum Standaardisatie
Van:	Bureau Forum Standaardisatie
Datum:	13 november 2020
Versie:	0.1
Bijlagen:	FS-20201209.4C2 **CONCEPT** Monitor Open Standaarden 2020 v0.9

Ter bespreking/akkoord

Duiding en Maatregelen Monitor Open Standaarden 2020
[Bijlage A Monitor Open Standaarden 2020]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met het volgende:

- De concept notitie duiding en maatregelen, t.a.v. het OBDO
- De Monitor Open Standaarden 2020 (eventuele majeure punten welkom)
- Zodat beide stukken kunnen worden doorgeleid naar het eerste OBDO van 2020 (ze zijn al opgesteld met het oog op die geadresseerde, exacte percentages, schema's + PM's zullen in aanloop naar het OBDO worden aangevuld)

Inleiding

De jaarlijkse Monitor Open Standaarden meet grofweg 3 dingen:

1. De naleving van de pas toe of leg uit verplichting in aanbestedingen: a) worden de relevante open standaarden van de pas-toe-of-leg-uit lijst uitgevraagd; en b) wordt er uitgelegd als dat niet is gedaan.
2. Hoe zit het met de toepassing van de pas-toe-of-leg-uit standaarden in de Voorzieningen en Afsprakenstelsels in de Gemeenschappelijke Digitale Infrastructuur (GDI), en enkele andere Rijksvoorzieningen.
3. Hoe zit het met het (meetbare) gebruik van de pas-toe-of-leg-uit standaarden bij de overheid.

Dit onderzoek wordt jaarlijks uitgevoerd door ICTU, in opdracht van het Forum Standaardisatie. ICTU heeft voor het onderzoek tevens ICT Recht, PBLQ en TNO ingezet.

Hoofdpunten en duiding

1. Voor wat betreft het vragen naar de juiste standaarden in de onderzochte aanbestedingen, valt op dat
    a. het percentage van aanbestedingen waarin om een of meerdere relevante standaarden wordt gevraagd weer verder is gestegen (95%). Dat is positief.
    b. Maar daar zit helaas een (weer) grotere groep aanbestedingen tussen, waarin maar om een enkele standaard is gevraagd, en waarbij belangrijke andere relevante standaarden zijn vergeten.
    Dat komt tot uiting doordat het percentage waarin om een relevante standaard is gevraagd weer terug is gevallen naar 45% [wat was dat percentage in Monitor 2019?].
    c. Dat er wederom in geen enkel jaarverslag is uitgelegd ('leg uit' deel van verplichting), indien is nagelaten om de standaarden toe te passen ('pas-toe' deel van verplichting). Niet bij de onderzochte aanbestedingen waarin verzuimt blijkt de relevante standaarden uit te vragen (ondanks aanschrijving daarover). Maar ook niet in andere gevallen.
    In een paar gevallen wordt in de bedrijfsvoeringparagraaf van het jaarverslag wel in algemene zin aandacht besteed aan de pas-toe-of-leg-uit standaarden, of verwezen naar detail informatie op een website (BZK verwijst naar het jaarverslag van Logius, waarin op de website de stand van zaken uitgebreid is opgenomen).

    [PM. Schema aanbestedingen door jaren heen invoegen]

2. Met ingang van dit jaar worden elk jaar wisselend een subset van het totaal aantal voorzieningen onderzocht. Dit jaar zijn de interactievoorzieningen onderzocht (inclusief 4 websites). Bij de toepassing van de standaarden in de voorzieningen en afsprakenstelsels valt op dat de groei doorzet. 91% voldoet helemaal, deels of heeft de implementatie gepland.

    [PM. Een schema t.a.v. voorzieningen invoegen]

3. Het beeld van het daadwerkelijk gebruik van standaarden, is divers. Niet bij alle standaarden kan het gebruik worden gemeten. Bij een beperkt aantal standaarden kan het gebruik **automatisch** worden gemeten. Opvallend is dat dat meten en publiceren een goede impuls lijkt te geven voor adoptie. Zeker in combinatie met een streefbeeldafspraak in het OBDO. De informatieveiligheid standaarden tegen phishing zijn daar een goed voorbeeld van. Dat lijkt ook te komen omdat het maatschappelijk nut van de standaarden duidelijk is: de noodzaak van informatiebeveiliging wordt inmiddels breed gevoeld en onderschreven.
    Toch is ook daar nog het nodige werk aan de winkel. Zo is het belangrijk ook de configuratie van de verschillende standaarden op orde te hebben. Een flink aantal overheidsdomeinnamen (in de meting van september 2020 nog 22%) loopt nog achter op het (aan de actuele dreigingen) aangepaste advies van NCSC. Verder is de configuratie van een anti-email-phishing standaarden nog steeds niet overal op orde. Valse e-mails uit naam van bijvoorbeeld bewindspersonen kunnen daardoor nog steeds bij burgers en bedrijven aankomen.

[PM. Een schema t.a.v. Gebruik toevoegen. Evt. IV-schema? Selectie paar web- en e-mail uitslagen, waaronder de problematische]

Maatregelen

1. Om te voorkomen dat de pas-toe-of-leg-uit standaarden worden ervaren als wéér een extra normenkader erbij, wordt verder gewerkt aan de vorig jaar aangekondigde vervlechting van de pas-toe-of-leg-uit standaarden in bestaande kaders. Zoals de kaders voor verslaglegging (Bedrijfsvoeringsparagraaf Rijksbegroting), inkopen en informatiebeveiliging (Baseline Informatiebeveiliging Overheid). Door die vervlechting wordt ook duidelijker wat de meerwaarde van de standaarden is, namelijk als instrument om te kunnen voldoen aan de principes uit bijvoorbeeld de BIO (beveiligingsplicht) of inkoop (leveranciers onafhankelijkheid). Die acties zijn reeds ingezet, maar moeten nog

met resultaat worden afgerond.

2. Adoptie van standaarden vindt natuurlijk plaats door de verschillende overheidsorganisaties zelf, en niet door het Forum Standaardisatie. Daarom is het van belang dat pas-toe-of-leg-uit bij organisaties zelf wordt geïnternaliseerd.

   Een van de kansrijke ontwikkelingen daarin is het op orde brengen van domeinnaamregie. Overheidsorganisaties hebben vaak geen idee welke website- en email domeinnamen zij bezitten en/of in gebruik hebben. Met het inrichten van *life-cycle* management, wordt voorkomen dat de wildgroei aan nieuwe websites en e-mail domeinen door blijft gaan[1], en dat domeinnamen in verkeerde handen vallen. Dat helpt ook burgers en bedrijven die door dat gebrek aan overzicht ook door de bomen het bos niet meer zien, en grote moeite hebben om publiek van privaat te onderscheiden, en bonafide van malafide. Met het goed inregelen van domeinnaamregie, kunnen ook de toepassing van de informatieveiligheidsstandaarden en digitale toegankelijkheid sterk worden verbeterd. Goede voorbeelden zijn het werk van AZ/DPC, de opschoon opdracht van de bestuursraad van VWS, een gelijksoortig project van CIO-BZK en de eerdere consolidatie van regio websites naar Politie.nl
   Het blijkt een goed effect te hebben wanneer deze pas-toe-of-leg-uit standaarden onderdeel gaan uitmaken van de i-Control functie van de CIO's. Dit illustreert dat het effectief is de adoptie van standaarden te vervlechten met andere kaders, waarbij het op te lossen maatschappelijk probleem of overheidsissue helder is.

3. Zoals afgesproken in het OBDO van begin 2020 is de monitor open standaarden en/of informatieveiligheid-meting besproken in verschillende overheidsgremia. Dat is nog niet in alle afgesproken gremia gebeurd, mede door de Corona-pandemie. Dat zal in 2021 alsnog gebeurden. Verder is het van belang er in die gremia periodiek op terug te komen. Ook dat zal worden ingepland.
   [PM Geupdate tabel met gremia en bezoekdata invoegen].

4. Een van de redenen waarom niet wordt uitgelegd, is het gebrek aan toezicht en handhaving. Er is niemand die erop aanslaat wanneer er niet wordt uitgelegd.
   Uit gesprekken met o.a. de ADR is duidelijk geworden dat haar taak in het kader van de Rijksbegroting niet per se toezicht op de Rijksinstructie betekent. Wel is samenwerking mogelijk op het gebied van informatieveiligheid (door bijv. hergebruik van iv-meting of gebruik van de bulkmeettool van internet.nl). Onderzocht zal worden op welke wijze wel aangestuurd kan worden op naleving van de Rijksinstructie. Daarbij wordt ook een opdracht tot onderzoek door de Rekenkamer overwogen.

5. Voor het aanjagen van de adoptie wordt ingezet op best practices, waarbij het maatschappelijk effect (meerwaarde) duidelijk wordt. De activiteiten van een aantal overheidsorganisaties rond Domeinnaamregie zoals hierboven genoemd, zijn daar een voorbeeld van.

6. Daarnaast is de combinatie van stimuleren en meetbare streefbeeldafspraken effectief. Bij de opname van nieuwe standaarden op de lijst, zal strenger bekeken worden of er (door bijvoorbeeld de indieners) ook aanpalend beleid/stimuleringsmaatregelen worden ondernomen.

Conclusie

Er is duidelijk te zien dat adoptie een kwestie is van lange adem. Het helpt om de problematiek keer op keer te agenderen in verschillende gremia van decentrale en centrale overheid, op zowel strategisch als tactisch en operationeel niveau. Dat is ook te zien aan het goede effect dat

[1] Een dergelijke ontwikkeling is ook privaat te zien. Coolblue is ook teruggekomen van individuele websites per product als scheerapparaat.nl en router.nl, en heeft nu alles geconsolideerd op coolblue.nl Ook Postnl.nl heeft 1 eenduidige e-mail domeinnaam.

streefbeeld afspraken, gecombineerd met periodiek meten, op termijn hebben. De eerste streefbeeldafspraken dateren uit 2015. Zij hebben een gestage toename tot gevolg. Op flink wat vlakken zijn we er bijna, maar er zijn nog wat laatste uitdagingen.

Duidelijk is verder te zien dat adoptie snel kan verlopen, als er voldoende urgentie wordt gevoeld. Begin dit jaar, werd ook in de media geconstateerd dat het e-mail adres @rivm.nl kwetsbaar was voor phishing of ander misbruik[2]. Binnen een dag is die kwetsbaarheid daarna verholpen. Dat gebeurde ook bij de e-mail domeinen @rijksoverheid.nl, en eerder bij o.a. @tweedekamer.nl, @aivd.nl en @rotterdam.nl, waarbij mensen namens politici en bestuurders konden mailen.

Het helpt wanneer de standaarden integraal onderdeel gaan uitmaken van het i-control beleid van de CIO's.

[2] Deze kwetsbaarheid kwam al gedurende een paar jaar in de halfjaarlijkse metingen aan het OBDO naar voren.