Duiding en Maatregelen Monitor Open Standaarden 2024

Vergadering:	Forum Standaardisatie 2 oktober 2024
Agendapunt:	4
Documentnummer:	FS-20241002.4A1
Aan:	OBDO en Ministerie van BZK
Van:	Bureau Forum Standaardisatie via Stuurgroep
Bijlagen:	Geen

Deze concept notitie is een oplegger bij de Monitor Open Standaarden 2024, waarin de resultaten uit de onderzoeken worden geduid, en verbetermaatregelen worden voorgesteld gericht aan het OBDO en -waar van toepassing- het Ministerie van BZK.

Na bespreking in het Forum gaan de onderzoeksrapporten, inclusief deze Duiding & Maatregelen notitie, onderweg naar het OBDO van 28 november 2024. Na behandeling in het OBDO stuurt de staatsecretaris van BZK de Monitor naar de Tweede Kamer.

In de vergadering van het Forum Standaardisatie van 2 oktober 2024 presenteerden de onderzoekers Siwert de Groot en Joost Vreuls de resultaten.

Duiding

De Monitor Open Standaarden gaat over de naleving van wetgeving en beleid dat van toepassing is op de lijst met verplichte open standaarden van het Forum Standaardisatie. Ook dit jaar is gekeken of het mogelijk is om de Monitor Open Standaarden bestuurlijk interessanter, korter en beter leesbaar te maken.

Het rapport ziet er daarom dit jaar als volgt uit:

- Het samenvattende document met hoofdlijnen en conclusies (ICTU)

- Het onderzoek naar de uitvraag van open standaarden bij aanbestedingen, en het onderzoek naar de naleving van het “Leg Uit” onderdeel in de jaarverslagen (ICTU)
- Het onderzoek naar de toepassing van de verplichte open standaarden in 27 landelijke voorzieningen (PBLQ)

Mede vanwege de omvang van het voorzieningenonderzoek, zullen het doorlopende onderzoek naar de gebruiksgegevens en de Ranking VAROS (Voldoen Aan Relevante Open Standaarden) op een later moment als zelfstandige publicatie worden geagendeerd. Op die wijze kunnen de actuele resultaten uit de Meting Informatieveiligheidstandaarden overheid medio 2024 daarin ook verwerkt worden.

Aanbestedingen

In het kader van de Monitor Open standaarden 2024 is voor het dertiende jaar op rij onderzoek gedaan naar de toepassing van open standaarden bij aanbestedingen door overheden, dit maal over aanbestedingen uit 2023. Daarbij gaat het om een steekproef bestaande uit 70 aanbestedingen. Per aanbesteding is vastgesteld welke open standaarden van de lijst daarop van toepassing waren en in hoeverre daar daadwerkelijk om is gevraagd ('pas toe'). In de 70 onderzochte aanbestedingen had in totaal 929 keer om een specifieke open standaard gevraagd moeten worden. Uit de aanbestedingsdocumenten en de eventuele correspondentie met aanbestedende diensten daarover, blijkt dat er 460 keer daadwerkelijk om de betreffende relevante standaard is gevraagd, ofwel: in 50 procent van de gevallen. Daarmee lijkt er sprake te zijn van stagnatie. Het uitvraag-percentage ligt namelijk sinds 2015 ruwweg rond de 45%. Tot nu toe is twee keer gepiekt boven de 50%, in 2021 voor het laatst.

Er wordt gedurende een lange periode dus gemiddeld om iets minder dan de helft van de relevante standaarden gevraagd, maar er zijn wel ieder jaar meer standaarden relevant. De toename van het aantal relevante standaarden per aanbesteding kan heel goed te maken hebben met een toename van het aantal uitgevraagde SAAS-applicaties, waarbij vooral de standaarden uit het domein ‘Veilig internet’ relevant zijn. Deze 15 standaarden (ruim een-derde van de lijst) zijn goed voor een belangrijk deel van het aantal keer relevant: in totaal was 929 keer een standaard relevant en daarvan betrof het 704 keer een standaard uit dit domein. Andere beeldbepalende domeinen zijn ‘Openbaar en toegankelijk’ en ‘Uitwisselingsfundament’. Door op deze drie domeinen aanvullende maatregelen te gaan nemen, zoals een wettelijke verplichting en meer inhoudelijke ondersteuning, kan de stagnatie mogelijk doorbroken gaan worden.

Wanneer we specifiek kijken naar de door het OBDO vastgestelde streefbeeldafspraken in het domein ‘Veilig internet’ dan zien we dat geen enkele standaard boven dat gemiddelde van 50% uitkomt. Bij DNSSEC gaat het om een percentage van 23%, SPF 29%, DKIM 30%, DMARC 26%, STARTTLS en DANE 22%, IPv6 39% en voor RPKI 4%. Voor RPKI verloopt de implementatie deadline eind dit jaar, voor de overige standaarden is deze al geruime tijd verlopen. Daarmee is duidelijk dat er voor deze standaarden verdergaande instrumenten moeten worden ingezet om aanbestedende diensten al tijdens het aanschafproces van ICT

producten en ICT diensten het gebruik of de ondersteuning van deze standaarden te laten uitvragen.

Wanneer we inzoomen op de open standaarden waarvan het gebruik nu al wettelijk verplicht is dan valt het volgende op:

Daar waar Digitoegankelijk relevant wordt geacht, ligt het uitvraag-percentage met 82% dit jaar fors hoger dan vorig jaar. Vrijwel alle aanbestedende diensten zijn al enkele jaren wettelijk verplicht om hun websites en mobiele applicaties toegankelijk te maken door toepassing van EN 301 549, en het is daarom verstandig om dit al tijdens de aanbesteding te eisen van leveranciers. In de aanbestedingen uit 2022 was nog sprake van een daling in de uitvraag, dus het is niet uitgesloten dat de start medio 2022 van het DigiToegankelijk toezichts- en ondersteuningsprogramma (DigiToegankelijk TOP) in positieve zin heeft bijgedragen aan de over 2023 geconstateerde hogere uitvraag.

Daar waar HTTPS en HSTS relevant worden geacht, ligt het uitvraag-percentage met 57% in 2023 echter juist fors lager dan het jaar eerder. Dit is opmerkelijk omdat het gebruik van deze standaarden vanaf 1 juli 2023 voor in ieder geval a-bestuursorganen wettelijk verplicht zijn geworden, en van de voorgeschreven toepassing niet mag worden afgeweken. Zelfs niet indien er sprake zou zijn van een onevenredige last. Het is moeilijk om zonder nader onderzoek te duiden waar deze daling door veroorzaakt is. Het kan er mee te maken hebben dat er in het voortraject van een aanbesteding van SaaS applicaties in het algemeen minder aandacht lijkt te zijn voor uit te vragen technische specificaties. Ook kan het te maken hebben met het ontbreken van voldoende praktische ondersteuning tijdens het inkoopproces, of door het nog niet aangewezen hebben van een toezichthouder. Uit aan het Bureau Forum Standaardisatie gestelde vragen is afgelopen jaar gebleken dat er organisaties zijn die weliswaar onder het organisatorische werkgebied voor de lijst met verplichte standaarden vallen, maar die niet een a-bestuursorgaan zijn. Denk bijvoorbeeld aan de AFM of aan ICTU. Het is daardoor in de communicatie onduidelijk (geworden) of zij op grond van de AMvB verplicht zijn deze standaarden uit te vragen en te gebruiken. Het is wenselijk om hier duidelijkheid over te verschaffen, een toezichthouder aan te wijzen op grond van artikel 17 Wet digitale overheid, en extra ondersteuning aan te bieden.

Jaarverslagen

Vervolgens is nagegaan in hoeverre overheden in hun jaarverslag verantwoording hebben afgelegd, wanneer bij aanbestedingen van de lijst werd afgeweken ('leg uit').

De Instructie rijksdienst geeft rijksbreed aan hoe bij de aanschaf van ICT diensten of producten te werk moet worden gegaan. De instructie moet in acht worden genomen door alle departementen en alle agentschappen. Daarbij verplicht artikel 4 om in de bedrijfsvoering paragraaf van het jaarverslag een verantwoording op te nemen over de toepassing van het beleid in de eigen organisatie, en om in het geval van specifieke afwijkingen een uitleg over die afwijking te geven. Het verplicht moeten hanteren van deze paragraaf is bovendien opgenomen in de Rijksbegrotingsvoorschriften.

Zeven van de twaalf departementen hebben een vorm van verantwoording opgenomen in het jaarverslag 2023. Bij de andere vijf departementen (Buza, EZK, Financiën, LNV en SZW) is in dit verband niets te vinden in het jaarverslag. Bij de eerstgenoemde vier had dat bovendien uitgebreider gemoeten omdat er in een onderzochte aanbesteding is afgeweken van het beleid.

In 2018 herbevestigde het OBDO de bestuurlijke afspraak dat ook andere overheidsorganisaties (waaronder de mede-overheden) in het jaarverslag blijvend moeten rapporteren over de wijze waarop zij bij de aanschaf van software en diensten omgaan met verplichte open standaarden. In de periode van 2011 tot 2022 is dit ook nog expliciet door de commissie BBV onder de aandacht gebracht in de richtlijnen voor provincies, gemeentes en waterschappen over de bedrijfsvoeringsparagraaf.

In de jaarverslagen van de onderzochte zbo's en de medeoverheden waarvoor 'leg uit' dit jaar noodzakelijk was, wordt echter over het beleid ten aanzien van open standaarden nergens gesproken, laat staan dat er een passage is gevonden die als een 'leg-uit' kan worden gezien.

Het ontbreken van een dergelijke passage wordt vermoedelijk veroorzaakt door onbekendheid met het beleid, en door het ontbreken van toezicht en sancties. Bovendien werkt aan de beeldvorming niet mee dat zelfs een aantal departementen zich niet houden aan dit voorschrift uit de Rijksinstructie. We moeten daarom constateren dat er in het geval van "Leg uit" al jaren geen sprake is van gedragsconformiteit.

Voorzieningen

Het beeld van de implementatie van verplichte open standaarden in de 27 onderzochte nationale voorzieningen is positief. Van de 488 relevante standaarden waren er 381 daadwerkelijk in voorzieningen toegepast, ofwel: 78 procent. Ten opzichte van de eerdere metingen uit 2021 en 2022 is dat een stijging. Als we ook meenemen dat voorzieningen soms deels voldoen aan de implementatie van de standaard of dat de implementatie gepland staat, dan is de score zelfs 95 procent. Kortom: bij de voorzieningen is in 2024 sprake van een hoog niveau van adoptie van verplichte open standaarden en van groei in vergelijking met het recente verleden.

Wel zijn er ook zorgen. Zo zijn er bij sommige voorzieningen ten opzichte van de eerdere metingen juist verslechteringen te zien waar het gaat om de voorgeschreven toepassing van wettelijk verplichte standaarden en standaarden waarvoor een streefbeeldafspraak bestaat: HTTPS en HSTS, IPv6, Digitoegankelijk, STARTTLS en Dane, en DNSSEC.

In veel gevallen heeft men er wel een uitleg voor gegeven, maar juist bij deze standaarden is afwijken van de regel niet meer toegestaan, en ook niet wenselijk.

Maatregelen

Om de geconstateerde stagnatie weer vlot te trekken zijn meerdere maatregelen noodzakelijk:

1. Een eerste stap is te zorgen dat men in meer organisaties überhaupt kennis heeft van het bestaan van het open standaarden beleid en de regelgeving. Neem daarvoor in bestuurlijke afspraken, bestuursakkoorden of een nieuwe Nationale Digitaliseringsstrategie nadrukkelijk de hantering van de verplichte en aanbevolen open standaarden op, en verwijs daarbij naar de lijsten van het Forum standaardisatie.
2. Schrijf beheerders van voorzieningen aan met de resultaten van de Monitor Open Standaarden en dring er voor zover de voorziening (nog) niet voldoet, op aan dat open standaarden worden opgenomen in de release planningen van die voorzieningen en in de "definition of done" bij organisaties met een Agile werkwijze.
3. Agendeer en bespreek in het OBDO die voorzieningen waarbij er in de afgelopen twee jaren een verslechtering is opgetreden waar het gaat om de voorgeschreven toepassing van wettelijk verplichte standaarden en standaarden waarvoor een streefbeeldafspraak bestaat.
4. Bereid zo snel mogelijk via de Wet Digitale Overheid voor alle acht standaarden waar eerder streefbeeldafspraken voor zijn gemaakt een AMvB voor waarin zowel het uitvragen alsook het gebruik van deze standaarden wettelijk verplicht worden. Kies daarbij voor een organisatorisch werkgebied dat breder is dan enkel a-bestuursorganen. Denk bijvoorbeeld aan het bij Digitoegankelijk gehanteerde criterium van "aanbestedende diensten".
5. Laat voor de domeinen 'Veilig internet', 'Openbaar en toegankelijk' en 'Uitwisselingsfundament' uitwerken op welke wijze toezicht en uitgebreidere ondersteuning kan plaatsvinden voor de verschillende doelgroepen binnen de overheid. Hanteer daarbij een benadering waarbij rekening wordt gehouden met voor de doelgroep relevante afwegingen.
6. Inventariseer of er uit eerdere jaren nog voorgestelde maatregelen ter hand genomen kunnen worden.