Notitie

Duiding en maatregelen Monitor Open standaarden 2018

FORUM STANDAARDISATIE woensdag 12 december 2018

Nummer:	FS 181212.4A1
Aan:	OBDO
Van:	Forum Standaardisatie
Betreft:	CONCEPT notitie van Forum aan OBDO
Datum:	30 november 2018
Versie:	Concept 0.4

De leden van het OBDO wordt gevraagd om:

- **In te stemmen met de duiding** van de Monitor Open standaarden 2018 van het Forum Standaardisatie en de hiermee verband houdende maatregelen, *danwel deze aan te vullen met uw eigen inzichten*;
- **Aan te sturen op het gebruik van de relevante pas-toe-of-leg-uit standaarden**, door:

    1. **De Monitor Open Standaarden 2018 te agenderen** in uw organisatie waar de onderzoeksresultaten relevant zijn.
    Denk hierbij niet alleen aan inkoopafdelingen en plaatsen waar ICT ontwikkeld en beheerd wordt (ICT-architecten en informatiebeveiligers), maar ook daar waar beleid ontwikkeld wordt met een sterke ICT component;

    2. **Achterblijvers in uw achterban aan te spreken**, bijvoorbeeld via de koepels, door het agenderen van de monitor inclusief iv-meting;

    3. **Aan te sturen op het opnemen van eventuele 'leg-uit' in het jaarverslag van uw organisatie**;

TOELICHTING

Duiding Monitor Open standaarden 2018

Inleiding

Het gebruik van de open standaarden van de pas-toe-of-leg-uit lijst van het Forum Standaardisatie in ICT systemen, is hard nodig om te komen tot een maatschappelijk relevante digitale overheid: veilig, betrouwbaar, onderling goed verbonden, niet te duur en stimulerend voor innovatie en marktwerking.

Het wordt steeds moeilijker uit te leggen waarom het gebruik van sommige van deze standaarden achterwege blijft. Vooral als het gaat om het niet tijdig implementeren van de internetveiligheidsstandaarden, kunnen situaties ontstaan die direct schadelijk kunnen zijn voor burgers en bedrijven, en slecht voor het imago van de overheid.

Zoals bijvoorbeeld in de zomer van 2018, toen circa 200 mensen slachtoffer werden van een phishing actie, waarbij domeinnamen van de overheid werden misbruikt. Hackers weken toen uit naar domeinnamen van de overheid, die de anti-phishing standaarden van de streefbeeldafspraken nog niet hadden ingevoerd.[1] Of denk aan het najaar van 2017 toen onbeschermde e-mailadressen van Tweede Kamer en AIVD vatbaar bleken te zijn voor misbruik.[2] Als tijdig de hiervoor relevante standaarden goed geïmplementeerd waren geweest, (zoals DNSSEC, DKIM, START TLS en DANE, TLS en SPF) hadden de gevolgen van de aanvallen kunnen worden beperkt.

Voor de internetveiligheidsstandaarden loopt de urgentie van het gebruik het meeste in het oog en het dan ook niet voor niets dat deze voorbeelden hier prominent genoemd worden. Maar voor *alle* open standaarden van de pas-toe-of-leg-uit lijst geldt dat ze gebruikt moeten worden. Discussie hierover is een gepasseerd station. Het is niet alleen de bedoeling van de *Instructie Rijksdienst voor de aanschaf van ICT-producten en ICT-diensten* (hierna verder: de Rijksinstructie), de strekking van de verplichting tot uitleggen in het jaarverslag (zoals bepaald in de Rijksbegrotingsvoorschriften) maar ook de aanhoudende wens vanuit de Tweede Kamer.[3]

Maar wat is de praktijk? Hoe staat het daadwerkelijk met het gebruik van de standaarden van de pas-toe-of-leg uit lijst door overheidsorganisaties? Dit onderzoek wordt jaarlijks in opdracht van het Forum Standaardisatie uitgevoerd door stichting ICTU, waarvan u bijgaand de meest recente versie aantreft: de Monitor Open standaarden 2018. Kort gezegd komen de resultaten op het volgende neer:

- Het aantal aanbestedingen waarin om open standaarden wordt gevraagd stijgt verder van 72% (2016) naar 81% (2017) tot 85% (2018). Daarbinnen neemt het percentage waarin om *alle* relevante open standaarden wordt gevraagd echter af: van 18% (2016) via 12% (2017) tot 6% (2018).
- Na 10 jaar leg-uit-verplichting komt het nog steeds zelden of nooit voor dat een overheidsorganisatie zich in het jaarverslag verantwoord over het niet-toepassen van een relevante standaard.
- De 35 onderzochte overheidsbrede voorzieningen voldoen in belangrijke mate aan de relevante open standaarden: van de 464 gevallen waarin een open standaard relevant was wordt in 70% van de gevallen daaraan voldaan en in 18% van de gevallen wordt deels voldaan of er zijn concrete plannen om er binnenkort aan te voldoen.[4]
- Het beeld van het gebruik van de standaarden verschilt: van 17 standaarden van de pas-toe-of-leg uit lijst is het beeld positief, van 8 is het beeld gemengd, en van 9 standaarden is het beeld negatief of onbekend.

[1] https://nos.nl/artikel/2239096-valse-mail-mijnoverheid-maakt-203-slachtoffers.html

[2] https://nos.nl/artikel/2199557-iedereen-kan-mailen-namens-de-aivd-dankzij-spoofing.html

[3] Zie p.9 en verder (Monitor Open standaarden 2018).

4 Zie ook p.3 van de Monitor Open standaarden 2018.

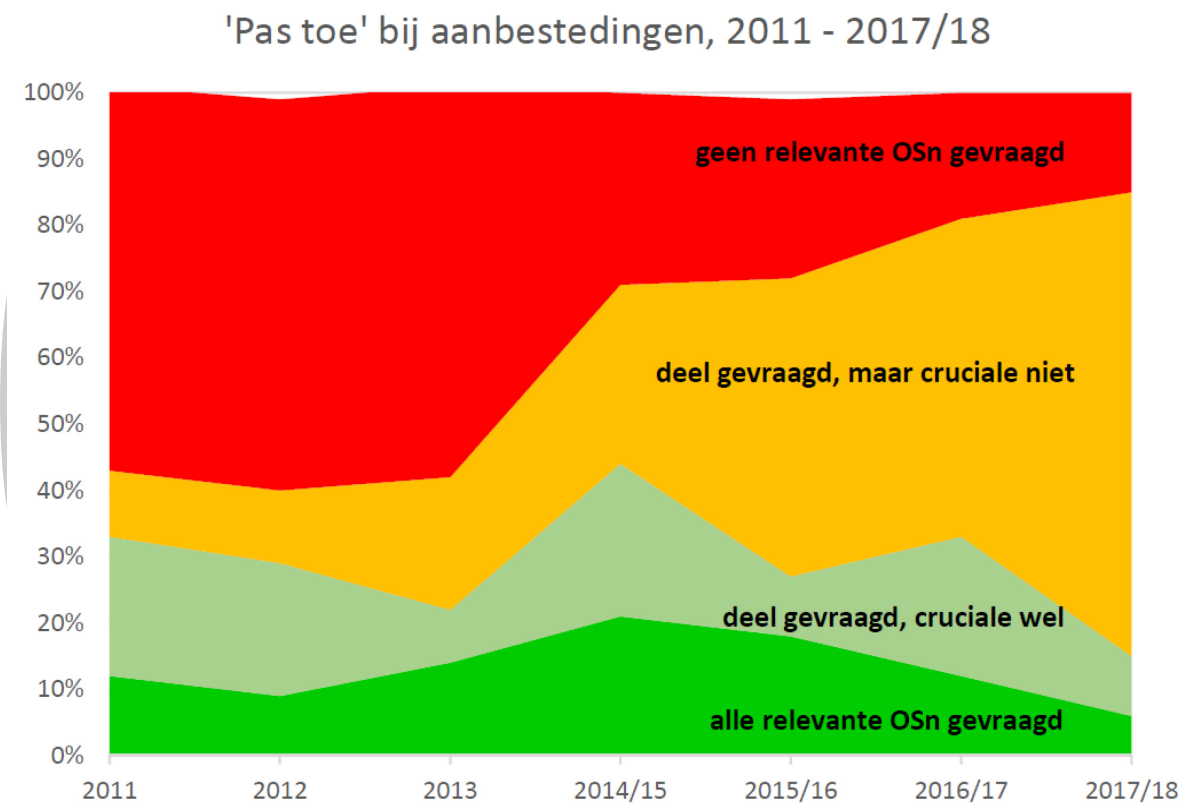
Deze notitie gaat verder over hoe het Forum Standaardisatie deze onderzoeksresultaten duidt en welke maatregelen zij hierop voorstelt aan het OBDO

Duiding Monitor open standaarden 2018

Aanbestedingen

Nog niet eerder was in aanbestedingen het percentage zo hoog dat gevraagd werd *om een deel* van de relevante open standaarden. Dat is positief.
Dat het percentage *alle relevante standaarden uitgevraagd* is gedaald, is echter zorgelijk en doet de vraag rijzen hoe dit komt.

Figuur 1. 'Pas toe' bij feitelijke aanbestedingen 2011 - 2017/2018 (Rijk en mede overheden samen)



Waarom is het percentage *alle relevante open standaarden uitgevraagd* achtergebleven? Hier zijn verschillende verklaringen voor:
Ten eerste was niet eerder het aantal aanbestedingen van medeoverheden zo groot. Deze groep scoorde op dit onderdeel van het onderzoek al langer minder goed dan overheidsorganisaties van het Rijk. Maar dit jaar was bij medeoverheden *geen enkele* aanbesteding te vinden waarbij *alle* relevante open standaarden waren uitgevraagd. Dat heeft het gemiddelde aantal aanbestedingen -waarin volledig naar alle open standaarden is gevraagd- danig naar beneden getrokken.
Ten tweede waren in 2018 meer open standaarden per aanbesteding relevant dan voorheen. Het was daarom ook moeilijker om ze *allemaal* in beeld te hebben.
Ten derde is het Forum Standaardisatie niet de enige organisatie die het gebruik van open standaarden predikt. Ook door andere organisaties wordt de bekendheid -en nut en noodzaak - van het gebruik van een aantal (met name informatieveiligheids) standaarden verspreid. Hierbij zijn de overige standaarden van de lijst- die ook verplicht zijn- niet of minder in beeld zijn. Dat andere organisaties open informatieveiligheidsstandaarden van de lijst- maar buiten de context van de lijst- naar voren brengen is uiteraard geen probleem. Sterker nog, het is een kans om op

aan te sluiten. Voorkomen moet wel worden dat de overige standaarden van de lijst ondersneeuwen.

Duiding 1. De pas-toe-of-leg-uit lijst en de Monitor Open standaarden zou bij de betrokkenen rond het moment van aanschaf van ICT meer en beter bekend mogen zijn. Met name bij ICT-architecten, inkopers,opdrachtgevers en leveranciers in de achterban van Forumleden en leden van het OBDO.

Leg uit in jaarverslagen

In de Rijksinstructie bij aanschaf van ICT-goederen en diensten, waarvan in het OBDO eerder is afgesproken dat die overheidsbreed zal worden toegepast, en in de Rijksbegrotingsvoorschriften staat een model voor het maken van een verantwoording over de bedrijfsvoering. Dit is het model dat gevolgd moet worden door organisaties die onder het Rijk vallen bij het maken van het jaarverslag. In de toelichting, onder het kopje financieel en materieel beheer staat onder punt 4:

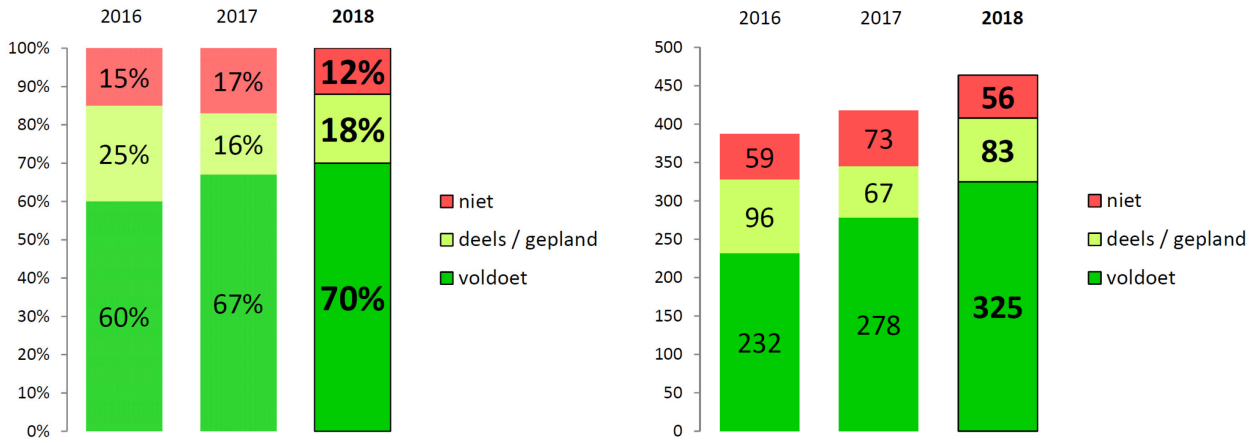
> In het onderdeel financieel en materieel beheer wordt vermeld als is afgeweken (het 'comply of explain'-beginsel) van artikel 3, eerste lid van de Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten). De Tweede Kamer wil dat de overheid meer gebruik maakt van open standaarden en open source software. De Instructie rijksdienst schrijft voor dat bij de aanschaf en ontwikkeling van ICT-diensten of ICT-producten in beginsel gebruik moet worden gemaakt van open standaarden van de lijst van het College Standaardisatie. Valide afwijkingsgronden zijn opgenomen in de Instructie Rijksdienst. Als er sprake is van afwijking van de Instructie Rijksdienst dan wordt dit gemotiveerd aangegeven.

Duiding 2. Uit de Monitor Open standaarden blijkt ook in 2018 weer dat de *leg-uit verplichting* zoals nu geregeld niet werkt. Na ruim tien jaar verplichten tot *leg-uit* komt het nog steeds niet tot zelden voor dat een overheidsorganisatie zich in het jaarverslag verantwoordt over het niet-toepassen van de relevante standaard(en). Het is tijd om ons te bezinnen op de vraag hoe de verplichting tot uitleggen gehandhaafd kan worden en wél tot uitleggen zou kunnen leiden.

Voorzieningen

Uit de Monitor Open standaarden 2018 komt het volgende beeld:

Figuur 2: Toepassing open standaarden in 35 voorzieningen: in % en absolute aantallen



Duiding 3 De adoptie van de relevante voorzieningen van de GDI verloopt goed. Waarschijnlijk draagt de wijze waarop het Monitoronderzoek wordt uitgevoerd ten aanzien van voorzieningen (jaarlijks contact tussen de onderzoekers en de beheerders) bij aan de adoptie van de relevante open standaarden. En ook het maken van de streefbeeldafspraken (en het meten hiervan ieder

half jaar) draagt waarschijnlijk bij aan het succes van de adoptie van de relevante open standaarden in voorzieningen. Doorgaan dus op deze weg.

Er zijn echter ook een aantal kritische kanttekeningen te plaatsen.
Ten eerste valt bij de toepassing van de relevante open standaarden in voorzieningen op dat vier standaarden slecht geadopteerd worden. Het gaat om CMIS, SKOS, IPv4 en IPv6 en Digikoppeling. De redenen hiervoor verschillen per standaard en verdienen extra aandacht.
Verder laat ook dit jaar de Monitor Open standaarden een scheiding zien in de 'pas toe of leg uit'-lijst, tussen aan de ene kant de groep standaarden waar redelijk veel over bekend is en die vaak relevant zijn in aanbestedingen en voorzieningen. Het gaat grofweg om de standaarden die vallen binnen de domeinen *Internet en beveiliging*, *Document & webcontent*, en *de Stelselstandaarden.*
Aan de andere kant zijn er de standaarden die niet of nauwelijks relevant blijken te zijn in aanbestedingen en voorzieningen. De onderzoekers krijgen op deze standaarden niet goed vat, of in ieder geval komt er vooralsnog weinig tot geen informatie over het gebruik uit naar voren. De doet de vraag rijzen hoe het gebruik van deze standaarden wél meer inzichtelijk gemaakt kan worden.

Duiding 4: Deze standaarden op de pas-toe-of-leg-uit-lijst zijn toe aan nadere beschouwing, waarin onder meer aandacht besteed wordt aan bovenstaande kanttekeningen.

De Monitor Open standaarden 2018 onderschrijft de koers die het Forum Standaardisatie al geformuleerd heeft haar werkplan van 2019 en de acties die hierin zijn opgenomen. Kort gezegd komt deze koers neer op:

- meer en beter communiceren van nut en noodzaak van het gebruik van de open standaarden van de pas-toe-of-leg uit lijst:
- partijen helpen de relevante open standaarden te selecteren en te gebruiken;
- de verplichting tot gebruik harder aanzetten met daarbij passende aandacht voor toezicht en handhaving.

De maatregelen die hierna in deze notitie voorgesteld worden zijn aanvullend op het werkplan van het Forum Standaardisatie, deels gericht tot de leden van het Overheidsbrede Beleidsoverleg Digitale Overheid, en deels een aankondiging van hetgeen door BZK, EZK en het Forum Standaardisatie zal worden onderzocht.

Het Forum Standaardisatie doet bij de voorgestelde maatregelen uitdrukkelijk het aanbod zo nodig ondersteuning te bieden.

Maatregelen

Naar aanleiding van de Monitor Open standaarden 2018 verzoekt het Forum Standaardisatie de leden van het Overheidsbrede Beleidsoverleg Digitale Overheid:

1. **De Monitor Open standaarden 2018 te agenderen** in uw organisatie waar de onderzoeksresultaten relevant zijn.

Denk hierbij in de eerste plaats aan inkoopafdelingen. Met name als het gaat om het communiceren van de lijst met onderzochte aanbestedingen.
Het Forum Standaardisatie zal gesprekken voeren met betrokkenen bij onderzochte aanbestedingen uit de Monitor Open standaarden en aanbestedende diensten notificeren zodra zij in beeld komen voor de Monitor Open standaarden 2019. Het zou goed zijn als inkoopafdelingen dan al bekend zijn met de Monitor Open standaarden.

Daarnaast vraagt het Forum Standaardisatie de Monitor Open standaarden te agenderen op de plaatsen waar ICT ontwikkeld en beheerd wordt (ICT-architecten & projectleiders, informatiebeveiligers)en waar opdrachtgevers werken. Vooral als uw organisatie voorzieningen beheert voor de Generieke Digitale Infrastructuur of een andere voorziening die onderzocht wordt in de Monitor Open standaarden.
Agendeer de Monitor open standaarden ook daar waar beleid ontwikkeld wordt met een sterke ICT

component. Geef mensen in uw organisatie hiermee tijdig aan rekening te houden met het implementeren van de open standaarden die reeds getoetst zijn op onder meer geschiktheid voor overheidsbreed gebruik door het Forum Standaardisatie.

2. **Met name achterblijvers in uw achterban aan te spreken**, bijvoorbeeld via de koepels, door het agenderen van de monitor inclusief iv-meting.

3. **Verantwoording op te nemen rond het gebruik van open standaarden in het jaarverslag van uw organisatie**.

Het Forum Standaardisatie vraagt de leden van het OBDO langs deze weg uitdrukkelijk zich te verantwoorden over het gebruik van de relevante open standaarden zoals aangegeven in de Instructie Rijksdienst voor de aanschaf van ICT-producten en ICT-diensten en de Rijksbegrotingsvoorschriften, waarvan in het OBDO is afgesproken ze overheidsbreed toe te passen. Of anders aan te geven waardoor naleving van de verplichting om dit te doen niet lukt, zodat naar andere wegen gezocht kan worden om de verantwoording gestalte te geven.

Daarnaast zal door BZK, EZK en het Forum Standaardisatie, bij de uitwerking van de NL Digibeter agenda worden onderzocht op welke wijze toezicht en handhaving vorm kan worden gegeven, in het kader van de daar genoemde – nog op te stellen – standaardisatieagenda[5]. Daarbij wordt ook gekeken wat de rol van de interne audit-diensten en aanbestedings-checklists kan zijn.

[5] P.50, https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2018/07/nl-digibeter-agenda-digitale-overheid.pdf