Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aanbiedingsformulier Overheidsbreed Beleidsoverleg Digitaal Overheid

1. Korte titel	Standaardisatie: Meting Informatieveiligheidstandaarden voorjaar 2022
2. Datum behandeling	22 september 2022
3. Aard van de behandeling: *(dubbelklikken op vakje en 'ingeschakeld' aanvinken)*	☐ Scrum ☐ Hamerstuk ☐ Ter besluitvorming ☒ Ter bespreking ☐ Ter kennisname ☐ Anders: …….
4. Eerder behandeld in:	☐ PL ☐ ICM ☐ MFG ☐ MT- DO i.o. **X** Anders: Forum Standaardisatie ☐ Niet Uitkomst behandeling in bovenstaand gremium: ☐ Overeenstemming *(geen toelichting vereist)*
5. Voorgeschiedenis / context *6. Samenvatting/ toelichting*	[bijlagen rapport en bijlage met individuele detailresultaten] **Overheidsbreed zijn afspraken gemaakt om moderne internetstandaarden voor websites en e-mail versneld te adopteren**. Forum Standaardisatie meet op verzoek van het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) halfjaarlijks de implementatievoortgang van deze afspraken. De afgesproken uiterlijke implementatiedata zijn voor alle standaarden al verstreken (eind 2019 voor de Informatieveiligheid standaarden & eind 2021 voor IPv6), waardoor verwacht mag worden dat alle webapplicaties en e-mailsystemen deze standaarden correct toepassen. In dit document wordt gerapporteerd over de stand van zaken per mei 2022. **Overheden die internetdomeinen niet veilig configureren nemen onnodige risico's.** Het gaat daarbij om een verhoogde kans op phishing uit naam van overheidsorganisaties, en een verhoogde kans op manipulatie en afluisteren van web- en e-mailverkeer. Een prominent voorbeeld van de gevolgen van onveilige configuratie van standaarden is een incident van e-mailphishing namens *@overheid.nl* in 2018, toen van 200 burgers DigiD-inloggegevens zijn buitgemaakt. Ook tijdens de Corona-crisis bleek dat cruciale domeinnamen van de overheid, zoals *rivm.nl* en *rijksoverheid.nl*, niet goed beschermd waren tegen spoofing. **De meting laat zien dat bij 53% van de internetdomeinen alle verplichte websitestandaarden correct zijn toegepast**. Het gaat om belangrijke beveiligingsstandaarden voor vertrouwelijk webverkeer, en IPv6 voor duurzame bereikbaarheid van online diensten.

	Bij 44% van de internetdomeinen zijn alle verplichte e-mailstandaarden correct toegepast. Hier gaat het om belangrijke beveiligingsstandaarden om e-mailvervalsing uit naam van de overheid te voorkomen en het e-mailverkeer vertrouwelijk te houden, en ook IPv6 voor duurzame bereikbaarheid van online diensten. **Met de meting zijn in totaal 2584 overheidsdomeinen gecontroleerd**. Dat is een uitbreiding ten opzichte van voorgaande metingen, in de voorgaande meting zijn 559 overheidsdomeinen gecontroleerd. De 2584 overheidsdomeinen zijn slechts een deelwaarneming van alle overheidsdomeinen, het totaalportfolio heeft vele duizenden meer domeinen. De overheid heeft als geheel geen zicht op het totaalportfolio. Dit rapport toont met diverse doorsnedes inzicht in de stand van zaken per overheidscategorie en per ministerie. De mate van adoptie kan gezien worden als een indicator voor de effectiviteit van sturing op kwaliteit van de informatievoorziening. Op verzoek van het OBDO is in de samenvatting een 'naming & shaming'-volgorde toegepast.
7. Beslispunten/ discussiepunten	Het OBDO neemt kennis van de 'Meting Informatieveiligheidstandaarden voorjaar 2022' en vraagt de CIO Rijk en de koepelorganisaties van de decentrale overheden om de rapportage en adviezen via de CISO- en de CIO-lijn actief onder de aandacht te brengen van individuele organisaties binnen hun achterban en hen op te roepen tot verbetering. Daarbij verzoekt OBDO aan de CIO Rijk en de koepelorganisaties om te onderzoeken hoe richting hun achterban voor de opvolging van de adviezen een stimulerende en faciliterende rol te kunnen vervullen en ook na te gaan welke (delen van de) adviezen overheidsbreed via de OBDO-lijn opgepakt zouden moeten worden (bijvoorbeeld via de lijn van de Architectuurraad). De CIO Rijk en de koepels van de decentrale overheden worden gevraagd in een volgend OBDO-overleg terug te koppelen over hun opvolging hierin. **Advies 1**: onderzoek welke sturingsmechanismen kunnen worden ingezet om overheidsbrede architectuurafspraken en kwaliteitseisen (beleid) – bijvoorbeeld in de vorm van gemeenschappelijke standaarden en streefbeeldafspraken – effectief te laten landen in de uitvoering bij de individuele overheidsorganisaties (implementatie). **Advies 2:** organiseer regie op internetdomeinen binnen ministeries en individuele overheidsorganisaties. Jaag dit initieel project- of programmamatig aan, en borg dit vervolgens in de lijnorganisatie. **Advies 3:** verken of het centrale dienstverleningsconcept rond DNS-beheer van de Rijksoverheid ook kan worden ingezet bij decentrale overheden. **Advies 4:** zorg ervoor dat naleving van IT-kwaliteitseisen – waaronder ondersteuning van verplichte open standaarden – onderdeel zijn van het leveranciersmanagement van individuele overheidsorganisaties. Vraag leveranciers periodiek naar de planning voor ondersteuning van standaarden. Overweeg om over te stappen als een leverancier onvoldoende meebeweegt.
8. Contactgegevens	1. Bart Knubben: 06-21162373 (inhoudelijk) 2. Joram Verspaget: 06-52845592 (proces)