Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Aanbiedingsformulier Overheidsbreed Beleidsoverleg Digitaal Overheid

1. Korte titel:	Standaardisatie: 02. Mutatie 'pas toe of leg uit'-lijst: verplichten van security.txt aan overheid
2. Datum behandeling:	OBDO: 25 mei 2023 (Strategisch Vooroverleg: 09 mei 2023)
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:*	Standaard security.txt (security- en policy-contactinformatie) te verplichten aan de overheid via plaatsing op de 'pas toe of leg uit'-lijst (veilig internet) [bijlagen 02a. Security.txt] De standaard security.txt draagt bij aan een veiliger internet doordat meldingen over kwetsbaarheden in een dienst of systeem sneller terecht komen bij de juiste personen binnen een organisatie. Op dit moment is er geen eenduidige wijze waarop een persoon of organisatie kwetsbaarheden in een systeem dat via http of https publiek benaderbaar is, kan melden bij de betreffende organisatie. Met security.txt komt een melding meteen op de juiste plek terecht. Hierdoor kunnen kwetsbaarheden sneller worden verholpen en is de kans kleiner dat cybercriminelen kwetsbaarheden gebruiken. De betrokken experts bij de toetsingsprocedure en reacties uit de openbare consultatie adviseren daarom om security.txt te verplichten aan de overheid (via 'pas toe of leg uit'-verplichting). Er is voldoende ervaring en draagvlak binnen de Nederlandse overheid voor security.txt. De standaard is laagdrempelig en eenvoudig (technisch) te implementeren, en is leveranciersonafhankelijk. De indieners van de standaard National Cyber Security Centrum (NCSC) en Digital Trust Center (DTC) hebben informatieproducten gepubliceerd

	voor overheden en bedrijfsleven, en hebben aangegeven voor meerdere jaren security.txt actief uit te dragen. Na de implementatie van de standaard blijft aandacht nodig voor de overheden voor het up-to-date houden van de informatie in het security.txt bestand en de inrichting van het achterliggende proces voor de juiste opvolging van een melding.
7. Beslispunten/discussiepunten:	Het OBDO stemt in met o standaard security.txt (security- en policy-contactinformatie) te verplichten aan de overheid via plaatsing op de 'pas toe of leg uit'-lijst (veilig internet)
8. Contactgegevens:	Hans Laagland (adviseur) [06-21820789]

02a. security.txt verplichten aan overheid (veilig internet)

Vergadering:	Overheidsbreed Beleidsoverleg Digitale Overheid donderdag 25 mei 2023 (SO OBDO 9 mei 2023)
Documentnummer:	02a.
Aan:	Overheidsbreed Beleidsoverleg Digitale Overheid
Van:	Forum Standaardisatie
Datum:	donderdag 25 mei 2023
Versie:	1.0
Bijlagen:	FS-20230412.3A-Forumadvies-security.txt

Ter besluitvorming

Forumadvies: security.txt verplichten aan overheid (‘pas toe of leg uit’-verplichting) (veilig internet)

Het OBDO stemt in om:

de standaard **security.txt** (security- en policy-contactinformatie) te verplichten aan de overheid (‘pas toe of leg uit’-verplichting) (veilig internet).

Advies en samenvatting

Het Forum Standaardisatie adviseert om de standaard **security.txt** te verplichten aan de overheid (‘pas toe of leg uit’-verplichting). security.txt is een standaard voor security- en policy-contactinformatie.

Op dit moment is er geen eenduidige wijze waarop een persoon of organisatie kwetsbaarheden in een systeem dat via http of https publiek benaderbaar is, kan melden bij de betreffende organisatie. Met security.txt komt een melding meteen op de juiste plek terecht.

Er is voldoende ervaring en draagvlak binnen de Nederlandse overheid voor security.txt. De standaard is laagdrempelig en eenvoudig (technisch) te implementeren, en is

leveranciersonafhankelijk. De indieners van de standaard National Cyber Security Centrum (NCSC) en Digital Trust Center (DTC) hebben informatieproducten gepubliceerd voor overheden en bedrijfsleven, en hebben aangegeven voor meerdere jaren security.txt actief uit te dragen. Na de implementatie van de standaard blijft aandacht nodig voor de overheden voor het up-to-date houden van de informatie in het security.txt bestand en de inrichting van het achterliggende proces voor de juiste opvolging van een melding.

Het Forumadvies geeft een nadere onderbouwing.

Belang van de standaard: veiliger internet

De standaard security.txt draagt bij aan een veiliger internet doordat meldingen over kwetsbaarheden in een dienst of systeem sneller terecht komen bij de juiste personen binnen een organisatie. Hierdoor kunnen kwetsbaarheden sneller worden verholpen en is de kans kleiner dat cybercriminelen kwetsbaarheden gebruiken. security.txt beschrijft op een uniforme wijze, hoe een kwetsbaarheid aan de betreffende organisatie gemeld kan worden.

Als sprake is van een kwetsbaarheid in een via http of https benaderbaar systeem, dan is snel handelen van enorme importantie. De kwetsbaarheid kan misbruikt worden om in te breken in het betreffende systeem en bijvoorbeeld databestanden met daarin persoonlijke gegevens te bemachtigen. Op dit moment is er geen eenduidige wijze waarop kwetsbaarheden gemeld kunnen worden bij organisaties die systemen hebben die bereikbaar zijn via http of https en verbonden zijn aan het internet.

Hoe is het proces verlopen?

National Cyber Security Centrum (NCSC) en Digital Trust Center (DTC) hebben op 2 juni 2022 security.txt aangemeld om te verplichten aan de overheid via plaatsing op de ‘pas toe of leg uit’-lijst. Op basis van het intakeadvies heeft het Forum Standaardisatie op 28 september besloten de aanmelding in procedure te nemen.

De expertgroep is op 19 januari 2023 bijeengekomen om de standaard te toetsen tegen de criteria en geïdentificeerde aandachtspunten te bespreken. Aan dit expertonderzoek namen vertegenwoordigers deel uit een brede coalitie van overheid, bedrijfsleven en koepelorganisaties.

Het Bureau Forum Standaardisatie publiceerde het expertadvies ter openbare consultatie op internetconsultatie.nl van 11 februari 2023 tot en met 12 maart 2023. Uit de openbare consultatie heeft het Bureau elf reacties ontvangen die hebben gereageerd op één of meer vragen uit de openbare consultatie. Reacties vroegen extra aandacht voor het up-to-date houden van de informatie in het security.txt bestand en voor de inrichting van het achterliggende proces voor de juiste opvolging van een melding, en attendeerden op de bestaande, internationale standaard WHOIS die deels hetzelfde doel heeft als security.txt.

Deze reacties zijn opgenomen in de eindconclusie in het Forumadvies. Dit Forumadvies is opgesteld op basis van het expertadvies, reacties uit de openbare consultatie en inzichten van de leden van het Forum Standaardisatie.

Het Forum Standaardisatie heeft op 12 april 2023 ingestemd met het Forumadvies.

Over de standaard

De standaard security.txt (*A File Format to Aid in Security Vulnerability Disclosure*) schrijft voor op welke wijze organisaties de gewenste securitycontactinformatie beschikbaar stellen. Wanneer een persoon of organisatie een kwetsbaarheid heeft gevonden in een systeem dat via http of https publiek benaderbaar is, dan kan eenvoudig de verantwoordelijke organisatie worden geïnformeerd door gebruik te maken van de beschikbaar gestelde contactinformatie via security.txt.

De standaard security.txt definieert een tekstbestand dat op een bekende locatie moet worden geplaatst. Het formaat van dit bestand kan door een machine worden geïnterpreteerd, zodat dit geautomatiseerd is te verwerken. Dit bestand is bedoeld om beveiligingsonderzoekers te helpen zo efficiënt mogelijk contact te zoeken met de verantwoordelijke personen van het betreffende systeem met betrekking tot beveiligingskwetsbaarheden.

De Internet Engineering Task Force (IETF) beheert de standaard onder de noemer RFC 9116.