Intakeadvies security.txt versie 1.0

Vergadering:	Forum Standaardisatie 28 september 2022
Agendapunt:	3
Documentnummer:	FS-20220928.3A-Intakeadvies-security.txt
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	28 september 2022
Versie:	1.0
Bijlagen:	geen
Rechten:	CC0 publieke domein verklaring

1 Samenvatting en advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om de standaard security.txt in procedure te nemen voor opname op de 'pas-toe-of-leg-uit' lijst. Een volledig expertonderzoek is aangewezen om de standaard te toetsen aan de criteria voor opname op de lijst.

Tijdens het intakegesprek hebben de indieners de wens geuit om de standaard in te dienen voor plaatsing op de 'pas-toe-of-leg-uit'-lijst. Tijdens het intakegesprek zijn de diverse criteria besproken. De standaard lijkt kansrijk om in aanmerking te komen voor plaatsing op de 'pas toe of leg uit'-lijst. Tijdens de expertbijeenkomst en het tot stand komen van het expertadvies zal extra aandacht zijn voor de volgende punten:

- Is het geven van een instructie aan de gebruikers van de standaard voldoende of is een Nederlands profiel noodzakelijk voor het toepassen van de standaard?
- Is er voldoende draagvlak bij de overheid voor het toepassen van deze standaard?
- Op welke wijze gaan de indieners van de standaard bijdragen aan de adoptie van de standaard?

In de rest van dit document wordt het advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 toetst in hoeverre de standaard voldoet aan

de criteria om in behandeling genomen te worden door het Forum Standaardisatie. Hoofdstuk 5 verkent of er inhoudelijke belemmeringen bestaan die een positief expertadvies in de weg zouden kunnen staan.

Tenslotte wordt er in hoofdstuk 6 een praktijkvoorbeeld gegeven dat Forum Standaardisatie kan gebruiken om de maatschappelijke waarde van de standaard te communiceren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

De standaard security.txt schrijft voor op welke wijze organisaties de juiste security- en policy-contactinformatie beschikbaar stellen. Wanneer een persoon of organisatie een kwetsbaarheid heeft gevonden in een dienst/systeem dat verbonden is aan het internet van een betreffende organisatie, dan kunnen eenvoudig de verantwoordelijken binnen de betreffende organisatie worden geïnformeerd door gebruik te maken van de beschikbaar gestelde contactinformatie via security.txt.

2.2 Waarom is deze standaard belangrijk?

Als sprake is van een kwetsbaarheid in een dienst of 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.

National Cyber Security Centrum (NCSC) en Digital Trust Center (DTC) zijn organisaties die als taak hebben de cyberweerbaarheid van de Nederlandse overheid en het bedrijfsleven te vergroten. Deze organisaties kunnen door gebruik te maken van de security.txt standaard veel sneller kwetsbaarheden melden bij de juiste personen binnen een organisatie. Hierdoor kunnen kwetsbaarheden sneller worden verholpen en is de kans dat kwetsbaarheden worden gebruikt door cybercriminelen kleiner. Dit leidt mede tot een veiliger internet en daarmee de bevordering van een veilige gegevensuitwisseling en informatieverstrekking.

3 Betrokkenen en proces

Op donderdag 2 juni 2022 meldden National Cyber Security Centrum (NCSC) en Digital Trust Center (DTC) de standaard security.txt formeel aan bij het Bureau Forum Standaardisatie middels het aanbieden van het ingevulde aanmeldformulier. Op maandag 20 juni 2022 heeft het intakegesprek plaatsgevonden. Bij het online intake gesprek waren de volgende personen aanwezig:

- Luitzen Homma (DTC)
- Christian Veenman (NCSC)
- Koen Sandbrink (NCSC)
- Hans Laagland (Bureau Forum Standaardisatie)
- Bart Knubben (Bureau Forum Standaardisatie)

- Robin Gelhard (Bureau Forum Standaardisatie)
- Arjen Brienen (Lost Lemon)
- Jeroen de Ruig (Lost Lemon)

In dit gesprek is onderzocht of security.txt voldoet aan de criteria om in procedure genomen te worden. Daarnaast is vooruitgeblikt op de procedure. Dit intakeadvies is tot stand gekomen op basis van de informatie in het aanmeldformulier en de aanvullend verkregen informatie tijdens het intake gesprek.

4 Voldoet de standaard aan de criteria om in procedure genomen te worden?

security.txt voldoet, zover we nu hebben kunnen vaststellen, aan alle vier de criteria om in behandeling genomen te worden voor plaatsing op de 'pas toe of leg uit'-lijst . Hoe de standaard is getoetst op de vier criteria wordt hieronder toegelicht in paragrafen 4.1-4.4.

4.1 Valt de standaard binnen de scope van Forum Standaardisatie?

De standaard is toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling. De standaard schrijft voor via welke kanalen en op welke wijze kwetsbaarheden kunnen worden doorgegeven met betrekking tot diensten/systemen die zijn verbonden met het internet. De kwetsbaarheden kunnen worden gemeld door overheidsorganisaties, bedrijven en burgers.

Daarnaast geeft het organisaties die toezien op de cyberweerbaarheid van overheden en bedrijven, zoals NCSC en DTC, de mogelijkheid om organisaties die (mogelijk) kwetsbaarheden hebben, snel te informeren over deze (mogelijke) kwetsbaarheden met eventueel te nemen maatregelen.

4.2 Heeft de standaard een toepassing die een enkele organisatie of sector overstijgt?

Het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard is voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid. De functionele toepassing van de standaard overstijgt het organisatorisch werkingsgebied van een enkele organisatie of sector.

De standaard is bedoeld voor alle organisaties die één of meerdere diensten/systemen hebben verbonden met het internet. De standaard is dus niet alleen bedoeld voor overheidsorganisaties, maar ook voor private ondernemingen. De gegevensuitwisseling die de standaard bewerkstelligt, is onder meer ten behoeve van de bevordering van de veiligheid van de gegevensuitwisseling en informatieverstrekking.

4.3 Is de standaard al wettelijk verplicht?

security.txt is niet wettelijk verplicht. De standaard draagt bij aan het beperken van cyberincidenten, door het zo effectief mogelijk informeren van organisaties. De verwachting is dat het opnemen van de standaard op de 'pas-toe-of-leg-uit'-lijst de adoptie van deze standaard zal versnellen.

4.4 Draagt de standaard bij tot de oplossing van een bestaand probleem?

Deze standaard draagt bij aan de oplossing van een bestaand en relevant probleem. Op dit moment is er geen eenduidige wijze waarop kwetsbaarheden gemeld kunnen worden bij organisaties die diensten/systemen hebben die verbonden zijn met het internet. Dit maakt het voor melders van cybersecurity kwetsbaarheden erg lastig om een kwetsbaarheid te melden bij de juiste personen binnen een organisatie. Dit is ook duidelijk toegelicht in het artikel "Security.txt wil orde brengen in de chaos van responsible disclosure". Deze standaard beschrijft op een uniforme wijze, hoe een kwetsbaarheid aan de betreffende organisatie gemeld kan worden.

De standaard is laagdrempelig en eenvoudig door iedere organisatie te implementeren en is hierdoor leveranciers onafhankelijk. Voor het Rijk is het CVD-proces centraal geregeld via NCSC. Dit betekent dat een gevonden kwetsbaarheid op een website of digitale dienst van de Rijksoverheid moet worden gemeld bij het NCSC. Daarnaast wordt er nagedacht over het invoeren van een centrale, gestandaardiseerde security.txt waar Rijksoverheden naar kunnen verwijzen.

5 Is er zicht op een positief expertadvies?

Als het Forum Standaardisatie de standaard in procedure neemt, gaat een groep experts de standaard toetsen op de vier inhoudelijke criteria voor opname op de lijst. Het Forum Standaardisatie neemt geen standaarden in procedure waarvan bij aanvang al vaststaat dat deze niet op een positief expertadvies kan rekenen. Daarom wordt in dit intakeadvies vooruitgeblikt op de vier inhoudelijke criteria.

Het intakeonderzoek heeft geen inhoudelijke criteria gevonden die een positief expertadvies voor plaatsing van security.txt op de 'pas toe of leg uit'-lijst in de weg zou kunnen staan.

Dit wordt toegelicht in paragrafen 5.1-5.4.

5.1 Toegevoegde waarde

De standaard security.txt heeft meerwaarde ten opzichte van andere standaarden met een (deels) overlappend functioneel toepassingsgebied. Deze standaarden staan overigens niet op de lijst van open standaarden. Er zijn enkele open standaarden die bijvoorbeeld voorschrijven op welke email-adressen of op welke wijze een kwetsbaarheid gemeld kan worden. Ook is het mogelijk om in de WHOIS data op te nemen op welk emailadres een kwetsbaarheid kan

worden gemeld. WHOIS is “een protocol om gegevens van een domeinnaam of IP-adres te achterhalen” (bron: Whois - Wikipedia).

In de WHOIS is vaak alleen de informatie van tussenliggende dienstverleners te vinden. security.txt heeft als voordeel dat eigenaar van het systeem of dienst zelf de mogelijkheid heeft om ook de security.txt-gegevens te onderhouden. Dit is bij WHOIS data moeilijker. Daarmee zijn de data die verkrijgbaar zijn via de standaard security.txt, doorgaans accurater. Er zijn geen vergelijkbare concurrerende open standaarden die eventueel in aanmerking komen voor plaatsing op de lijst van open standaarden.

security.txt is opgebouwd uit verschillende andere open standaarden. De security.txt moet bijvoorbeeld worden aangeboden via HTTPS en in txt-formaat.

Er zijn enkele risico’s verbonden aan het gebruik van de standaard. Bij juiste toepassing van de standaard, zijn deze risico’s beperkt. Belangrijk advies in de implementatie van security.txt is om niet te verwijzen naar individuele personen, maar naar algemene emailadressen en telefoonnummers i.v.m. AVG en privacyregels. Daarnaast is de standaard eenvoudig te implementeren en zijn hier nauwelijks kosten aan verbonden. De baten kunnen groot zijn doordat NCSC en/of DTC snel de juiste kanalen kunnen vinden om bij een kwetsbaarheid te waarschuwen. Het inbreken in een systeem kan namelijk grote financiële en privacy consequenties hebben.

5.2 Open standaardisatieproces

De specificaties van de standaard zijn vrij toegankelijk. Het beheer en de doorontwikkeling van de standaard is belegd bij de Internet Engineering Task Force (IETF); IETF is een onafhankelijke organisatie. IETF heeft als kernwaarden dat het tot stand komen van een standaard een open proces is en dat IETF voor iedereen die geïnteresseerd is, de mogelijkheid wil bieden bij te dragen aan de standaarden die IETF beheert. Het beheerproces is transparant en publiek benaderbaar en iedere belanghebbende kan participeren in het beheerproces. Er is ook een bezwaarprocedure.

Voor de Nederlandse overheid is er in principe geen aanvullend belang ten opzichte van andere partijen om de standaard te implementeren. NCSC vertegenwoordigt de Nederlandse overheid in de doorontwikkeling van de standaard. NCSC staat positief tegenover het gebruik van security.txt door overheidspartijen. Het NCSC is het centraal meldpunt voor kwetsbaarheden van Rijksoverheidspartijen.

Partijen die bijdragen aan de ontwikkeling van de standaard, leveren deze bijdrage *royalty free* en zullen geen beroep doen op intellectueel eigendomsrecht. Er is een regeling met betrekking tot het bijdragen van organisaties aan de ontwikkeling van door IETF ontwikkelde en beheerde standaarden met betrekking tot intellectueel eigendomsrecht.

Er is binnen Nederland nog geen organisatie die ondersteuning biedt bij de implementatie van de standaard. De standaard is relatief eenvoudig te implementeren. Mogelijk valt te denken aan een nationaal instructiefilmpje die toelicht hoe je de standaard implementeert.

De IETF bestaat sinds 1986. De IETF geeft inzicht in de eigen financiële situatie. Er is geen reden om aan te nemen dat IETF binnen drie jaar niet meer in staat is de standaard te beheren en door te ontwikkelen. Bovendien wordt de verdere ontwikkeling vormgegeven door een levendige community van vrijwilligers die zich inzetten de standaard verder te verbeteren.

5.3 Draagvlak

De standaard wordt inmiddels toegepast door honderden overheidssites in binnen en buitenland. Enkele voorbeelden:

- Nationaal Cyber Security Centrum (NCSC)
- Digital Trust Center (DTC)
- Rijksoverheid
- Belastingdienst

Er is geen onderzoek gedaan naar het draagvlak voor de standaard binnen de overheid. Het feit dat veel overheidssites de standaard al hebben geïmplementeerd, geeft aan dat er draagvlak is voor de standaard. Deze toets zal ook nog verder plaatsvinden tijdens de expertbijeenkomst en expertonderzoek.

De standaard is *backwards compatible*. Er is zover bekend geen *compliancy tool* beschikbaar om de *compliance* te testen. Voorstel van de indieners is om de standaard onderdeel te maken van internet.nl, een *compliancy tool* voor meerdere internet standaarden waar ook het Bureau Forum Standaardisatie nauw bij betrokken is.

Op dit moment is niet bekend of eerdere versies van de standaard ook daadwerkelijk geïmplementeerd zijn binnen de overheid. De indieners hebben wel aangegeven dat zij op- en aanmerkingen hebben op de huidige versie en hierover in gesprek zijn met IETF en dat dit kan leiden tot een nieuwe versie. Een belangrijke *request for change* is een aanvulling voor subdomeinen. Sommige organisatie willen onderscheid kunnen maken tussen een hoofddomein en eventuele subdomeinen met betrekking tot security.txt.

Volgens de indieners is er geen Nederlands profiel nodig voor het toepassen van de standaard, hoogstens wat spelregels die heel goed kunnen worden toegelicht in een promotie/uitleg filmpje. Denk bijvoorbeeld aan de regel dat je geen persoonlijk emailadres opneemt, maar een gezamenlijk niet tot een persoon te herleiden emailadres. Zo zijn er nog een paar spelregels te bedenken die de toepassing van de standaard nog effectiever maken. Tijdens de eventuele expertsessie moet getoetst worden of de andere experts daar ook zo over denken en welke behoefte er nog meer is om de adoptie en gebruik van de standaard te stimuleren.

De standaard is eenvoudig te implementeren. De indieners hebben ter indicatie gesproken met een Internet Service Provider (ISP), die voor klanten de standaard kan implementeren. Kosten zijn beperkt. De inrichting van de CVD procedure, onder andere het goed afhandelen van meldingen, kan wel de nodige kosten met zich meebrengen.

5.4 Opname op de lijst bevordert adoptie

Plaatsing van de standaard op de ‘pas toe of leg uit’-lijst, zal zorgen voor meer bekendheid van de standaard en daardoor zullen overheidsorganisaties de standaard gaan implementeren of weloverwogen toelichten waarom ze dit niet doen. Een blijvende, actieve rol van DTC en NCSC is daarbij van cruciaal belang. In de expertadvies fase zal worden onderzocht of de indieners voldoende plannen hebben om de adoptie van de standaard te vergroten.

6 Praktijkvoorbeeld

Hieronder een voorbeeld van de implementatie van security.txt op de website van Inspectie Justitie en Veiligheid. Deze implementatie geeft een persoon/organisatie die een kwetsbaarheid heeft gevonden voldoende informatie om te weten hoe de kwetsbaarheid kan worden gemeld.

```
# This is a security.txt file following https://securitytxt.org/
# If you discover any weaknesses or vulnerabilities on this website,
# please report this via our Policy URL (see below)
# to the National Cyber Security Centre (NCSC)
# A report like this is called a Coordinated Vulnerability Disclosure (CVD).
# We will discuss the issue with the NCSC and resolve it as soon as possible.
# We thank you in advance for helping us making our product better and more secure!
Contact: mailto:cert@ncsc.nl
Preferred-Languages: nl, en
Policy: https://english.ncsc.nl/contact/reporting-a-vulnerability-cvd
Policy: https://www.ncsc.nl/contact/kwetsbaarheid-melden
Expires: 2022-09-01T00:00:00.000Z
```