Expertadvies security.txt

Aan:	Forum Standaardisatie
Van:	Lost Lemon
Datum:	9 februari 2023
Versie:	1.0
Bijlagen:	n.v.t.

1 Samenvatting en advies

De experts die betrokken waren bij het expertonderzoek, adviseren om security.txt op te nemen op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie.

Het voorgestelde functioneel toepassingsgebied voor security.txt is:

> *security.txt moet worden toegepast op alle systemen die via http of https publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is.*

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 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.

Tijdens de intakefase van de standaard is een paar punten benoemd die in dit expertonderzoek nader worden bekeken:

- aandacht voor een implementatierichtlijn (in relatie tot een eventueel op te stellen Nederlands profiel)
- aandacht voor draagvlak bij de overheid voor het toepassen van deze standaard

- aandacht voor stimuleren van adoptie van de standaard

In de rest van dit document wordt dit advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van het nut en de werking van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 geeft de samenstelling van de expertgroep weer. Hoofdstuk 5 documenteert hoe de experts de standaard beoordelen tegen de criteria voor opname op de lijst.

Tenslotte geeft hoofdstuk 6 aanvullende adviezen van de experts aan het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) om de adoptie van de standaard te stimuleren.

2 Korte beschrijving van de standaard

2.1 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, 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 deze 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 standaard is laagdrempelig en eenvoudig te implementeren en is hierdoor leveranciersonafhankelijk.

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

2.2 Waarom is deze standaard belangrijk?

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.

Als sprake is van een kwetsbaarheid in een middels 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. Dit maakt het voor melders van cybersecurity kwetsbaarheden erg lastig om een kwetsbaarheid te melden. Dit is ook duidelijk toegelicht in het artikel "Security.txt wil orde brengen in de chaos van responsible disclosure". security.txt beschrijft op een uniforme wijze, hoe een kwetsbaarheid aan de betreffende organisatie gemeld kan worden.

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 en hebben de standaard ingediend bij het Bureau Forum Standaardisatie. Ook deze organisaties kunnen door gebruik te maken van de security.txt standaard veel sneller kwetsbaarheden melden bij de juiste persoon binnen een organisatie. Hierdoor kunnen kwetsbaarheden sneller worden verholpen en is de kans dat kwetsbaarheden worden gebruikt door cybercriminelen kleiner.

3 Betrokkenen en proces

Op donderdag 2 juni 2022 hebben Luitzen Homma (DTC) en Christian Veenman (NCSC) security.txt aangemeld voor plaatsing op de 'pas toe of leg uit'-lijst.

Op maandag 20 juni heeft een intakegesprek plaatsgevonden met de indieners, de procedurebegeleider en Bureau Forum Standaardisatie. In dit gesprek is onderzocht of security.txt voldoet aan de criteria om in procedure genomen te worden. De resultaten van het onderzoek zijn vastgelegd in het intakeadvies. Op basis van dit intakeadvies heeft het Forum Standaardisatie op 28 september 2022 besloten de aanmelding in procedure te nemen.

Hierop volgend heeft de procedurebegeleider in overleg met de indieners en Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld.

De leden van de expertgroep hebben een concept expertadvies gekregen dat is opgesteld met informatie uit de aanmelding en het intake onderzoek. Voorafgaand aan de expertbijeenkomst heeft de expertgroep dit concept expertadvies doorgenomen en aandachtspunten geïdentificeerd.

De expertgroep is op donderdag 19 januari 2023 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten uit de intakefase in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld. Dit expertadvies geeft de uitkomst van de expertgroep weer.

Het Bureau Forum Standaardisatie publiceert dit expertadvies ter openbare consultatie op internetconsultatie.nl van 11 februari tot en met 12 maart. Gedurende deze consultatieperiode kan iedereen op het expertadvies reageren. Na afsluiting van de openbare

consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep. Indien nodig kan dit aanleiding geven tot een aanvullend expertonderzoek.

Het Forum Standaardisatie formuleert op basis van het expertadvies, reacties uit de openbare consultatie en inzichten van de leden van het Forum Standaardisatie zelf een advies aan het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). Het OBDO besluit om het advies wel of niet over te nemen.

4 Samenstelling van de expertgroep

Forum Standaardisatie streeft naar een representatieve expertgroep met een evenwichtige publiek-private vertegenwoordiging van (toekomstige) gebruikers, leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertbijeenkomst leidt.

Aan de expertbijeenkomst hebben deelgenomen:

- Luitzen Homma (DTC) **(indiener)**
- Christian Veenman (NCSC) **(indiener)**
- Gerrit Berkhouwer (Ministerie van Algemene Zaken)
- Hayo Bethlehem (Ministerie van Algemene Zaken)
- Theo van Diepen (Logius)
- Frank Breedijk (DIVD)
- Remko Sikkema (VNG-R)
- Marco Davids (SIDN)
- Alex Gleusteen (Enable-U)
- Sijma Sabunchi (Ministerie van Volksgezondheid, Welzijn en sport)
- Ralph Moonen (Secura)
- Kees van de Maarel (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)

Als onafhankelijk voorzitter zou optreden Bas van Luxemburg (directeur van Lost Lemon). Vanwege zijn afwezigheid hebben beide procesbegeleiders deze rol overgenomen.

Jeroen de Ruig (Adviseur) en Arjen Brienen (Adviseur) bij Lost Lemon, hebben de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Hans Laagland, Benjamin Broersma en Wouter Kobes van het Bureau Forum Standaardisatie waren als toehoorders bij de expertbijeenkomst aanwezig.

5 Toetsing op inhoudelijke criteria

Het Forum Standaardisatie hanteert vier hoofdcriteria om te bepalen of een standaard in aanmerking komt voor opname op de lijst:

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?

4. Is opname op de lijst nodig om de adoptie te bevorderen?

Ieder van deze hoofdcriteria heeft deelcriteria die beschreven staan op de website van het Forum Standaardisatie. Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing.

5.1 Toegevoegde waarde

Met dit criterium wordt bepaald of het toepassingsgebied van de standaard duidelijk is, of deze zich goed verhoudt tot andere standaarden die al dan niet op de lijst staan, of de standaard een duidelijke meerwaarde heeft en of deze opweegt tegen eventuele risico's en nadelen.

5.1.1 Waardering van het criterium criteria 'Toegevoegde waarde'

De experts komen tot de conclusie dat security.txt voldoet aan het criterium 'toegevoegde waarde'. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.1.2 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

5.1.2.1 Is het functioneel toepassingsgebied goed gedefinieerd?

Het voorgestelde functioneel toepassingsgebied voor security.txt op de 'pas toe of leg uit' lijst is:

> *security.txt moet worden toegepast op alle systemen die via http of https publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is.*

Na enige discussie wordt met de experts gekomen tot bovenstaande formulering van het functioneel toepassingsgebied. Dit is voldoende duidelijk en beschrijft eenduidig het verplichte gebruik van de standaard (zowel websites als een 'kaal IP'). Gekozen is voor deze formulering omdat dit het meest recht doet aan waarvoor de standaard bedoeld is en daarmee ook duidelijk is voor de verantwoordelijken binnen een organisatie betrokken bij de inkoop dat voorzieningen die aan deze standaard moeten voldoen.

5.1.2.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Het voorgestelde organisatorisch werkingsgebied voor security.txt op de 'pas toe of leg uit'-lijst is:

> *Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.*

Dit is het gangbare organisatorisch werkingsgebied voor standaarden op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. De experts hebben de wens om hier expliciet de term ZBO aan toe te voegen omdat het vermoeden bestaat dat de huidige formulering voor ZBO's onvoldoende duidelijk is dat de standaard ook voor hen van toepassing is.

5.1.2.3 Is de standaard generiek toepasbaar?

De standaard kan over de grenzen van organisaties of sectoren gebruikt worden, en is niet alleen bedoeld voor gegevensuitwisseling binnen één organisatie of sector.

5.1.3 Verhoudt de standaard zich goed tot andere standaarden?

5.1.3.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast?

De experts stellen vast dat de standaard een relatie heeft met de standaarden https en DNSSEC. De standaard https wordt genoemd in het functioneel toepassingsgebied om zo goed mogelijk te duiden waar de standaard op van toepassing is. Er is geen overlap met het functioneel toepassingsgebied van deze standaard en het gegeven dat beide standaarden op de 'pas toe of leg uit'-lijst staan, heeft geen verdere impact. Tot slot wordt DNS security TXT genoemd. DNS security TXT is een standaard in ontwikkeling en complementair aan security.txt.

5.1.3.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied?

Niet van toepassing. De experts stellen vast dat de standaard geen relaties heeft met andere standaarden op de lijst. De standaard wordt juist gezien als complementair.

5.1.3.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname?

Wel wordt WHOIS genoemd als mogelijk alternatief, maar deze kent in de praktijk minder betrouwbare contactinformatie. WHOIS is een protocol om gegevens van een domeinnaam of IP-adres te achterhalen door middel van een query/vraag aan een database. In een WHOIS staan meestal de naam en contactgegevens van de eigenaar, de provider en nameservers van de DNS-servers.

Middels security.txt kom je direct bij de verantwoordelijke security-officer uit, met WHOIS vaak bij de eigenaar van de website. WHOIS is daarom niet granulair genoeg om direct bij de verantwoordelijke van het systeem uit te komen die belast is met het verwerken van security issues. WHOIS komt volgens de experts niet in aanmerking om opgenomen te worden op de Lijst Open Standaarden van het Forum Standaardisatie.

Een andere standaard die wordt genoemd door de experts, is RFC 2142. Deze standaard regelt de afspraken met betrekking tot generieke bereikbaarheid van domeinnamen via e-mail en is niet specifiek gericht op security. Daarnaast is er RFC 1035 Start Of Authority (SOA). Het DNS 'start of authority'-record (SOA) slaat belangrijke informatie op over een domein of zone, zoals het e-mailadres van de beheerder, wanneer het domein voor het laatst is bijgewerkt en hoe lang de server moet wachten voor een nieuwe refresh. Alle DNS-zones

hebben een SOA-record nodig om te voldoen aan de IETF-normen. Ook deze standaard is niet specifiek gericht op security.

5.1.3.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden?

Ja, de standaard is door de IETF als *informational* RFC opgenomen als open standaard.
De IETF kent verschillende categorieën van open standaarden. In geval van security.txt gaat het om een *informational* standaard.

5.1.4 Wegen de voordelen van de standaard op tegen de nadelen?

5.1.4.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?

Ja, de kosten van implementatie worden acceptabel geacht. De standaard implementeren vraagt weinig tijd en is relatief eenvoudig te realiseren. Het inregelen van het proces om te zorgen dat de juiste security.txt is opgenomen en dat de gegevens hierin altijd up tot date zijn, is een grotere inspanning dan de eenmalige implementatie.

Een door de indieners benaderde provider is gevraagd naar de extra kosten voor implementatie en beheer van security.txt per systeem. De provider heeft aangegeven te denken aan een bedrag van EUR 99,00 per jaar, met de mogelijkheid voor afnemen aanvullende dienstverlening voor het verwerken/ triage van meldingen via een maandelijkse fee (EUR 7,00). De experts ervaren dit bedrag als hoog voor de inspanning die de provider hiervoor moet leveren. De kosten van een hack zijn uiteraard veel hoger.

5.1.4.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?

Nee, deze is niet aanwezig. De experts geven aan dat de kosten van een datalek of een hack van het systeem heel hoog zijn, dus het loont de moeite om security.txt te implementeren, zeker gezien de inspanning die het kost om de standaard te implementeren.

5.1.4.3 Is de meerwaarde van de standaard goed inzichtelijk te maken?

De meerwaarde van de standaard is goed inzichtelijk te maken. De standaard draagt bij aan het voorkomen van een veiligheidsprobleem. 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.

5.1.4.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, de beveiligingsrisico's worden door de experts acceptabel geacht. Het is belangrijk dat security.txt op een systeem niet zelf gehackt wordt. De kwetsbaarheden van een systeem

komen dan binnen bij de hacker en dan is het voor de hacker eenvoudig om binnen te dringen in het systeem.

Aan de implementatie van RFC 9116 zitten uiteraard ook enkele security overwegingen die een organisatie moet afwegen bij de implementatie van deze standaard. Deze zijn terug te vinden in de RFC. Een hacker kan bijvoorbeeld bij een hack van de website de security.txt file aanpassen en zijn eigen emailadres hierin opnemen. De kwetsbaarheden van de applicatie of website komen dan binnen bij de hacker zelf.

5.1.4.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, de privacyrisico's worden door de experts acceptabel geacht.

Op de contactkanalen die gespecificeerd worden in de security.txt kunnen uiteraard wel privacyaspecten van toepassing zijn. Een voorbeeld hiervan is als er een persoonlijk e-mailadres wordt toegepast als kanaal om kwetsbaarheden te melden. In RFC 9116 wordt enkele malen het voorbeeld gebruikt om security@ als email adres te gebruiken, zoals ook beschreven in RFC 2142 section 4. Implementatieadvies is dus om geen persoonlijk emailadres op te voeren in security.txt. Ook moet worden opgelet met forwards naar personen die op vakantie zijn of langdurig ziek. Deze worden dan ontvangen door degene die een melding doet.

5.2 Open standaardisatieproces

Met dit criterium wordt bepaald of het beheer en de (door)ontwikkeling van de standaard op een open, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.

5.2.1 Waardering van het criterium criteria 'open standaardisatieproces'

De experts komen tot de conclusie dat security.txt voldoet aan het criterium 'open standaardisatieproces'. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.2.2 Is de documentatie voor een ieder drempelvrij beschikbaar?

5.2.2.1 Is het specificatiedocument zonder belemmeringen beschikbaar?

Ja, de specificatie van de standaard is publiek en vrij toegankelijk.

5.2.2.2 Is de documentatie over het ontwikkel- en beheerproces beschikbaar zonder dat er sprake is van belemmeringen?

Ja, de standaard wordt door IETF beheerd en het volledige proces van tot stand komen en doorontwikkeling van de standaard is transparant en publiek benaderbaar.

5.2.3 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

5.2.3.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard onherroepelijk royalty-free voor eenieder beschikbaar?

Ja, de IETF stelt het intellectueel eigendomsrecht op security.txt onherroepelijk en royalty-vrij voor iedereen beschikbaar. IETF biedt mogelijkheid voor vastleggen van auteursrecht. In de praktijk is nog geen gebruik gemaakt van deze mogelijkheid. Tot het moment van opstellen van dit expertadvies is er geen claim gelegd.

5.2.3.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht voor (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar stellen?

Ja, zie hiervoor de volgende beschrijving van IETF.

5.2.4 Is de inspraak van eenieder in voldoende mate geborgd?

5.2.4.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden?

Ja, het betreft het besluitvormingsproces van IETF.

5.2.4.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?

Ja, het betreft het besluitvormingsproces van IETF.

5.2.4.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?

Ja, de IETF heeft hiervoor een adequate bezwaarprocedure.

5.2.4.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?

Ja, het betreffen de standaardisatieprocedures van IETF.

5.2.4.5 Organiseert de standaardisatieorganisatie een openbare consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?

Ja, het betreffen de standaardisatieprocedures van IETF.

5.2.5 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

5.2.5.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?

Ja, bij de IETF.

5.2.5.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?

Ja, de standaard wordt beheerd door de IETF.

5.2.6 Is het (versie) beheer van de standaard goed geregeld?

5.2.6.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard?

Ja, de IETF heeft dergelijk gepubliceerd beleid.

5.2.6.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?

Ja, de beheerdocumentatie is goed vindbaar en te bekijken op internet.

5.2.6.3 Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?

De Nederlandse overheid is niet betrokken, maar de procedures van IETF bieden hiervoor wel de mogelijkheid.

5.2.6.4 Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?

Ja, de IETF heeft hiervoor adequate vertegenwoordiging.

5.2.6.5 Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?

De procedures van het IETF zijn goed geregeld. Het IETF is echter een internationale organisatie. De Nederlandse aanmelders van de standaard hebben geen invloed op de beheerprocessen van de betreffende organisatie, waardoor geen sprake kan zijn van de kwalificatie 'uitstekend beheer' voor de aanmelders. Dit betekent dat een eventuele nieuwe versie van de standaard ter toetsing moet te worden aangeboden aan het Forum Standaardisatie.

5.2.7 Is er adoptieondersteuning voor de standaard?

5.2.7.1 Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?

Hiervoor kan men terecht bij de community: IETF maillinglists of security.txt Github. Verder kunnen DTC en NCSC als goede bronnen voor onafhankelijke informatie geraadpleegd worden. Zo heeft DTC een uitgebreide instructie beschikbaar gesteld.

Verder onderhouden de auteurs van de standaard een website waar tools en meer informatie wordt aangeboden m.b.t. security.txt. Er is geen werkgroep meer, deze wordt opgeheven als

de standaard gereed is. Er is nog wel een communitygroup waar kan worden gediscussieerd over de standaard, wat eventueel kan leiden tot een nieuwe versie van de standaard. De experts vertrouwen erop dat met deze inrichting van een communitygroup het beheer voldoende is geborgd.

5.2.7.2 Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?

Ja, op de website van security.txt wordt een security.txt generator aangeboden. Ook DTC promoot de standaard, heeft onlangs een parser en validator beschikbaar gesteld waarmee kan worden gecontroleerd of de ingevoerde gegevens voldoen aan de structuur van security.txt. Tot slot heeft het NCSC implementatierichtlijnen opgesteld en een voorbeeldtekst voor security.txt opgesteld voor gebruik voor het opstellen van een eigen, op de eigen organisatie toegesneden tekst.

In de testtool Internet.nl is een test opgenomen die test of de website voldoet aan security.txt. De experts doen een oproep aan NOREA (beroepsorganisatie van IT-auditors) om organisaties die audits uitvoeren, mee te geven dat zij aandacht hebben voor security.txt tijdens de audits. Voor gemeenten overweegt de Informatiebeveiligingsdienst (IBD) van VNG-R om ondersteuning te bieden aan gemeenten bij de implementatie van security.txt. De aanwezige experts juichen dat toe.

5.3 Draagvlak

Met dit criterium wordt bepaald of de opname van de standaard op de 'pas toe of leg uit' lijst of lijst aanbevolen standaarden op voldoende draagvlak kan rekenen over de breedte van de overheid. Een voorwaarde hiervoor is ook dat er voldoende marktondersteuning voor de standaard bestaat, en dat het marktaanbod evenwichtig is (dus geen leveranciersafhankelijkheid in de hand werkt).

5.3.1 Waardering van het criterium criteria 'draagvlak'

De experts komen tot de conclusie dat security.txt voldoet aan het criterium 'draagvlak. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.3.2 Bestaat er voldoende marktondersteuning voor de standaard?

5.3.2.1 Bieden meerdere leveranciers ondersteuning voor de standaard?

De implementatie van de standaard is eenvoudig en mede daarom is er voldoende marktondersteuning voor de implementatie van de standaard. De experts vragen zich af in hoeverre grote softwareleveranciers voldoende genegen zijn security.txt te implementeren op hun diensten. Gemeentes zijn juist afnemer van diensten van deze grote partijen.

Volgens metingen van SIDN zijn er binnen Nederland 75.000 websites en systemen voorzien van security.txt (websites van zowel overheid als private websites); dit is 1,4% van domeinnamen met een actieve website.

5.3.2.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?

Ja, DTC heeft een parser beschikbaar gesteld, waarmee *compliancy* kan worden vastgesteld. Inmiddels is de standaard ook onderdeel van de testsuite van Internet.nl. Internet.nl beoordeelt of security.txt is geïmplementeerd op een middels http of https benaderbaar systeem.

5.3.2.3 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?

Ja, de standaard biedt voldoende interoperabiliteit. Aanvullende standaardisatieafspraken (zoals lokaal profiel) zijn niet nodig voor implementatie van security.txt.

5.3.2.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?

Ja, er zijn handreikingen en factsheets beschikbaar, opgesteld door het NCSC. In de handreiking staat een voorbeeldimplementatie en ook op example.nl is een voorbeeld beschikbaar. Meer dan 75.000 websites (1,4% van domeinnamen met een actieve website) kunnen fungeren als voorbeeldimplementatie van de standaard security.txt, waaronder ook voorbeeldimplementaties van Nederlandse overheden, zoals van Inspectie Justitie en Veiligheid.

5.3.3 Kan de standaard rekenen op voldoende draagvlak?

5.3.3.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?

De experts van dit expertadvies zijn vertegenwoordigers van verschillende overheidsorganisaties, zoals Logius, VNG en verschillende Ministeries. Allen onderstrepen het belang van deze standaard en geven aan deze standaard te willen implementeren. De vraag is of provincies en waterschappen zich ook voldoende bewust zijn van het belang van deze standaard. Hierbij geldt ook dat NCSC als entry-point voor de overheid kan dienen; decentrale overheden zullen zelf op individueel niveau of in een samenwerkingsverband dit moeten richten. Dit is wel een aandachtspunt.

5.3.3.2 Staan de overheidsorganisaties die worden geraakt door een verplichting van de standaard achter het verplichte gebruik van de standaard?

Ja, zie pa. 5.3.3.1. DTC heeft op zijn community, waar meer dan 1400 IT-professionals zoals CISO en ISO's actief zijn, een topic gemaakt over deze standaard. Uit dit topic kwamen geen noemenswaardige bezwaren naar voren.

5.3.3.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Ja, experts geven aan op basis van metingen van de testtool Internet.nl dat iets minder dan 20% van de overheidswebsites op moment van opstellen van dit expertadvies een valide security.txt-bestand heeft (binnen .nl-websites is het adoptiepercentage 1,4%). Dit betekent dat er ervaring aanwezig is binnen de Nederlandse overheid met de implementatie van security.txt.

Enkele Nederlandse voorbeelden:

- implementatie van security.txt op de website NCSC
- implementatie van security.txt op de website Digitaltrustcenter
- implementatie van security.txt op de website Rijksoverheid
- implementatie van security.txt op de website Belastingdienst

5.3.3.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Niet van toepassing, er is geen formele eerdere versie van de standaard. Er zijn wel eerdere *drafts* die al zijn geïmplementeerd door organisaties. De eerdere *drafts* zijn compatible met de eerste formele versie van security.txt. Voor deze organisaties is security.txt te beschouwen als voortzetting en doorontwikkeling.

5.3.3.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

Niet van toepassing, er is geen formele eerdere versie van de standaard. Zie ook het antwoord bij 5.3.3.4.

5.3.3.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?

Ja, veel grote partijen hebben de standaard al geïmplementeerd (zie ook pa. 5.3.3.3). De experts zien voldoende positieve signalen voor toekomstig gebruik. NCSC is voornemens te acteren als entry-point, hetgeen een drempel kan wegnemen bij overheidsorganisaties om security.txt te gaan gebruiken. Er is minder zicht op voorgenomen gebruik door provincies en waterschappen. Dit is een aandachtspunt (zie ook pa. 5.3.3.1).

Verschillende prominente cyber security influencers hebben aandacht besteed aan deze standaard, zoals Brian Krebs en Troy Hunt.

5.4 Opname op de lijst bevordert adoptie

De experts komen tot de conclusie dat security.txt voldoet aan het criterium ‘opname op de lijst bevordert adoptie’. Zowel DTC als NCSC geven aan de adoptie van security.txt te gaan

voortzetten na opname van de standaard op de ‘pas toe of leg uit’-lijst door continuering van de al ingezette activiteiten rond ondersteuning in de adoptie en de implementatie van de standaard (zie ook pa. 5.2.7.2).

Verplichting van de standaard verhoogt de veiligheid van overheidswebsites doordat bekend is waar en hoe kwetsbaarheden gemeld kunnen worden. Mochten organisaties toch besluiten hiervan af te wijken, dan doen zij dit weloverwogen en goed onderbouwd.

6 Adviezen bij opname van de standaard

De experts geven het Forum Standaardisatie en OBDO de volgende adviezen bij plaatsing van security.txt op de ‘pas toe of leg uit’ lijst:

- NCSC en DTC: de oproep aan de aanmelders van de standaard (NCSC en DTC) om meerjarig de standaard te promoten en ondersteuning bieden aan overheidsorganisaties (regierol aan de Nederlandse overheid).
- NCSC en DTC: de oproep aan de aanmelders van de standaard (DTC en NCSC) om met een handreiking te komen voor het inrichten van processen rond het beheer van de standaard binnen je eigen organisatie nadat de standaard is geïmplementeerd (ten behoeve van verankering van de standaard binnen een organisatie).
- NCSC: de oproep aan het NCSC om security.txt op te nemen in de volgende versie van de 'ICT-beveiligingsrichtlijnen voor webapplicaties'.
- Forum Standaardisatie: de oproep aan Forum Standaardisatie om VNG op te roepen om een campagne te starten naar de gemeenten en gemeentelijke leveranciers toe en ondersteuning te bieden bij de implementatie van security.txt.
- Forum Standaardisatie: de oproep aan Forum Standaardisatie om aan het organisatorisch werkingsgebied expliciet de term ZBO toe te voegen. De experts vermoeden dat in de huidige formulering het voor ZBO’s onvoldoende duidelijk is dat de standaard ook voor hen van toepassing is.
- (Semi)overheidsorganisaties: de oproep aan (semi)overheidsorganisaties die de standaard implementeren, om zoveel mogelijk gebruik te maken van bestaande tooling voor mogelijkheden om kwetsbaarheden te melden en dit op te nemen in de security.txt (zoals een webformulier en API in plaats van een e-mailadres).
- (Semi) overheidsorganisaties: de oproep aan (semi)overheidsorganisaties die de standaard implementeren, om de implementatie tenminste in te richten op het hoofddomein.
- De Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken: de oproep aan de Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken die domeinnamen uitgeeft voor overheidswebsites, om de implementatie van security.txt in algemene instructies bij nieuwe websites en domeinnamen mee te nemen.
- Logius: de oproep aan Logius om in het normenkader van DigiD security.txt op te nemen.

- Basisbeveiliging: de oproep aan Basisbeveiliging om check in te bouwen voor de standaard security.txt en hiervoor afstemming te zoeken met DTC en Internet.nl
- SIDN: de oproep aan SIDN om het gebruik van de standaard door overheidsorganisaties te meten en hiervoor een extra filtering (op overheidswebsites) te ontwikkelen binnen de eigen toolset.
- NOREA: de oproep aan NOREA om aan organisaties die audits uitvoeren, mee te geven aandacht te hebben voor security.txt tijdens de audits.