Forumadvies security.txt versie 1.0

Vergadering:	Forum Standaardisatie 12 april 2023
Agendapunt:	3
Documentnummer:	FS-20230412.3A-Forumadvies-security.txt
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Bijlagen:	20230209-Expertadvies-security.txt-v.1.1 Reacties uit de openbare consultatie van security.txt
Rechten	CC0 publieke domein verklaring

1 Advies

Het Forum Standaardisatie adviseert om de standaard 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'

Er is er 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. Extra aandacht is nodig 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.

In de rest van dit document wordt dit advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van het belang van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam en de experts die daarbij betrokken waren. Hoofdstuk 4 beschrijft de resultaten van de toetsing van de standaard tegen de criteria voor opname op de lijst.

Tenslotte geeft hoofdstuk 5 aanvullende adviezen 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 wat 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 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 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. 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.

3 Betrokkenen en proces

3.1 Gevolgde procedure

National Cyber Security Centrum (NCSC) en Digital Trust Center (DTC) hebben op 2 juni 2022 security.txt aangemeld om security.txt te verplichten aan de overheid via plaatsing op de ‘pas toe of leg uit’-lijst. De procesbegeleiders hebben op 20 juni 2022 een intakegesprek gevoerd

met de indieners. De procesbegeleiders hebben een intakeadvies opgesteld dat de resultaten van het intakeonderzoek documenteert.

Op basis van het intakeadvies heeft het Forum Standaardisatie op 28 september besloten de aanmelding in procedure te nemen. Hierop hebben de procedurebegeleiders in overleg met de indieners en Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld. Paragraaf 3.2 geeft de samenstelling van de expertgroep weer.

De expertgroep is op 19 januari 2023 bijeengekomen om de standaard te toetsen tegen de criteria en geïdentificeerde aandachtspunten te bespreken. Tijdens deze bijeenkomst zijn ook het functioneel toepassingsgebied en organisatorisch werkingsgebied voorgesteld. De uitkomst van het expertonderzoek is vastgelegd in een expertadvies.

Het Bureau Forum Standaardisatie publiceerde het expertadvies ter openbare consultatie op internetconsultatie.nl van 11 februari 2023 tot en met 12 maart 2023.

Dit Forumadvies is opgesteld op basis van het expertadvies, reacties uit de openbare consultatie en inzichten van de leden van het Forum Standaardisatie zelf. Indien het Forum Standaardisatie instemt met dit advies, wordt het aan het OBDO ter besluitvorming voorgelegd.

3.2 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 Berkouwer (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 Bas van Luxemburg (directeur van Lost Lemon) optreden. Vanwege zijn afwezigheid hebben beide procesbegeleiders deze rol overgenomen. Jeroen de Ruig en Arjen Brienen (beiden senior consultant van Lost Lemon) hebben de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

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

3.3 Resultaat van het expertonderzoek

De geconsulteerde experts hebben geadviseerd om de standaard security.txt op te nemen op 'pas toe of leg uit'-lijst. Experts hebben aangegeven dat extra aandacht nodig is 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. Deze aandachtspunten komen ook naar voren uit de reacties uit de openbare consultatie (zie pa. '3.4 Resultaat van de openbare consultatie'). De experts hebben verschillende adviezen gegeven (zie hoofdstuk '5 Adviezen bij opname van de standaard').

3.4 Resultaat van de openbare consultatie

In de openbare consultatie werden elf reacties ontvangen (waarvan tien reacties zijn gepubliceerd), waaronder de volgende personen en organisaties:

- Dhr. P. Wouters te Toronto (Canada)
- G.J. Meeuwisse te Delft van eerlijkdigitaalonderwijs.nl
- ETS Jonker te 's Hertogenbosch van Internet Cleanup Foundation
- Floor Terra te Amersfoort

De overige personen die hebben gereageerd, hebben kenbaar gemaakt te willen reageren zonder publicatie van persoonsgegevens. Een aantal suggesties uit de reacties zijn verwerkt in de adviezen bij hoofdstuk '5 Adviezen bij opname van de standaard'.

Van de elf ontvangen reacties zijn twee uitgesproken positieve ondersteuningen, drie met opmerkingen zonder blokkerende bezwaren (geen tegenstanders) en vier tegenstanders van het verplichten van security.txt aan de overheid via plaatsen op de 'pas toe of leg uit'-lijst. Vanwege het aantal reacties zijn deze gegroepeerd op de inhoudelijke onderdelen.

De tegenstanders van de verplichting zien het creëren van nog een extra locatie voor contactgegevens als nadelig en zien WHOIS of DNS (SOA-record) als goed alternatief (zie voor relatie met andere standaarden: pa 4.1 Toegevoegde waarde). Eén reactie benoemde veiligheidsrisico's en suggereerde dat een goed onderhouden contact e-mailadres op de homepage een beter alternatief is. Verder wordt het achterhaald raken van de gegevens uit security.txt genoemd als nadeel.

Het gebruik van een (persoonlijke) mailadres wordt in drie reacties genoemd als risico voor spam of het adresseren van de verkeerde persoon. De expertbijeenkomst benoemde deze risico's ook: in pa. 5.1.4.5 van het Expertadvies wordt het gebruik van persoonlijke e-mailadressen daarom afgeraden.

DNS security TXT wordt als alternatief genoemd in een reactie.

Er zijn twee suggesties gedaan (o.a. van eerlijkdigitaalonderwijs.nl) ter verduidelijking van (http) redirects. Floor Terra adviseert om de omschrijving van het Policy-veld in de standaard

op te nemen zodat “security.txt niet kan worden gebruikt om eenzijdig voorwaarden op te leggen aan de melder”. DTC en NCSC kunnen deze suggesties overnemen.

De reacties bevatten ook suggesties voor verbetering van de standaard. Zo heeft eerlijkdigitaalonderwijs.nl voorgesteld naast een veld ‘Hiring’ ook een veld ‘Volunteering’ toe te voegen en om optioneel een veld Policy toe te voegen. Deze suggesties kunnen worden ingebracht bij de beheerorganisatie IETF.

Verder werden er in een aantal reacties gewezen op hoe organisatorisch om te gaan met Coordinated Vulnerability Disclosure (CVD)-meldingen. Een security.txt kan niet bestaan zonder een CVD-beleid. Het is daarom belangrijk om een CVD-beleid op orde te hebben.

Eén reactie betrof de effectiviteit van het ‘pas toe of leg uit’-beleid in het algemeen.

4 Toetsing op inhoudelijke criteria

Het Forum Standaardisatie hanteert vier criteria 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 een passend middel om de adoptie te bevorderen?

Op de website van het Forum Standaardisatie is informatie te vinden over deze criteria en de toetsingsprocedure.

Dit hoofdstuk beoordeelt in hoeverre de standaard security.txt voldoet aan deze vier criteria op basis van het expertadvies, de reacties uit de openbare consultatie en de inzichten van de leden van het Forum Standaardisatie.

4.1 Toegevoegde waarde

De toetsingsprocedure wijst uit dat security.txt voldoet aan het criterium ‘toegevoegde waarde’.

De standaard heeft een relatie heeft met de standaarden https en DNSSEC op de ‘pas toe of leg uit’-lijst. Er is geen overlap met het functioneel toepassingsgebied van https met security.txt. Daarnaast wordt DNS security TXT genoemd. DNS security TXT is een standaard in ontwikkeling en complementair aan security.txt.

security.txt is complementair aan bestaande standaarden die niet op de ‘pas toe of leg uit’-lijst staan. Het gaat hier om WHOIS, RFC 2142 (afspraken met betrekking tot generieke bereikbaarheid van domeinnamen via e-mail) en RFC 1035 (DNS 'start of authority'-record (SOA) slaat belangrijke informatie op over een domein of zone). RFC 2142 en RFC 1035 zijn niet specifiek gericht op security.

WHOIS wordt gezien als alternatief voor security.txt. 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. Via security.txt kom je direct bij de verantwoordelijke security-officer uit met WHOIS vaak bij de eigenaar van de website. WHOIS is niet granulair genoeg om direct bij de verantwoordelijke van het systeem uit te komen belast met het verwerken van security issues.

De kosten van implementatie worden acceptabel geacht. Het inregelen van het proces om te zorgen dat de juiste security.txt is opgenomen en dat de gegevens hierin altijd up-to-date zijn, is een grotere inspanning dan de eenmalige implementatie. Een security.txt kan niet bestaan zonder een CVD-beleid. Het is daarom belangrijk om een CVD-beleid op orde te hebben.

De standaard heeft meerwaarde. 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.

De beveiligingsrisico's worden door de experts acceptabel geacht. Het is belangrijk dat security.txt op een systeem niet zelf gehackt wordt. Van belang is het advies om geen aan personen te relateren informatie op te nemen in het txt-bestand en om de gegevens in security.txt up-to-date te houden.

4.2 Open standaardisatieproces

De toetsingsprocedure wijst uit dat security.txt voldoet aan het criterium 'open standaardisatieproces.

Het beheer en de doorontwikkeling van de standaard is belegd bij Internet Engineering Task Force (IETF). Dit is een internationaal gerenommeerde beheerorganisatie voor standaarden die volledig voldoet aan de daarvoor gestelde eisen vanuit de toetsingsprocedure voor open standaarden.

Voor meer informatie over de standaard kan men binnen Nederland terecht bij de community: IETF maillinglists of security.txt Github. DTC en NCSC kunnen als goede bronnen voor onafhankelijke informatie geraadpleegd worden. Zo heeft DTC een uitgebreide instructie beschikbaar gesteld en heeft NCSC een handreiking gepubliceerd met meer informatie over de standaard en hoe die toegepast kan worden

Er is binnen de IETF geen werkgroep meer voor security.txt, deze wordt opgeheven als de standaard gereed is. Er is nog wel een communitygroup waar kan worden gediscussieerd over de standaard, hetgeen eventueel kan leiden tot een nieuwe versie van de standaard. De experts vertrouwen erop dat met deze inrichting van de communitygroup het beheer voldoende is geborgd.

4.3 Draagvlak

De toetsingsprocedure wijst uit dat security.txt voldoet aan het criterium ‘draagvlak.

De standaard is laagdrempelig en eenvoudig (technisch) te implementeren en is leveranciersonafhankelijk. Er is voldoende marktondersteuning voor de implementatie van de standaard. Een gebruiker kan de conformiteit van de implementatie van de standaard toetsen middels een door DTC beschikbaar gestelde parser.

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. Volgens metingen van SIDN zijn er binnen Nederland 75.000 websites en systemen voorzien van security.txt (websites van zowel overheid als private websites); zij kunnen fungeren als voorbeeld-implementatie van de standaard security.txt, waaronder ook voorbeeldimplementaties van Nederlandse overheden, zoals van Inspectie Justitie en Veiligheid.

De experts die aanwezig waren op de expertbijeenkomst van 19 januari 2023, 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. Veel grote partijen hebben de standaard al geïmplementeerd. De experts zien voldoende positieve signalen voor toekomstig gebruik. De vraag is of provincies en waterschappen zich ook voldoende bewust zijn van het belang van deze standaard. NCSC kan dienen als entry-point voor de rijksoverheid; decentrale overheden zullen zelf op individueel niveau of in een samenwerkingsverband dit moeten richten. Dit is een aandachtspunt.

4.4 Opname op de lijst bevordert adoptie

De toetsingsprocedure wijst uit dat security.txt voldoet aan het criterium ‘opname op de lijst bevordert adoptie’.

Verplichting van de standaard via ‘pas toe of leg uit’-verplichting verhoogt de veiligheid van overheidswebsites doordat bekend is waar en hoe kwetsbaarheden gemeld kunnen worden.

5 Adviezen bij opname van de standaard

Het Forum Standaardisatie geeft de volgende adviezen bij plaatsing van security.txt op de ‘pas toe of leg uit’-lijst:

1. aan de koepel- en netwerkorganisaties binnen de overheid, zoals CIO-Rijk, het Centrum Informatiebeveiliging en Privacybescherming (CIP), het Interprovinciaal Overleg (IPO), de Unie van Waterschappen (UvW) en Vereniging van Nederlandse Gemeenten (VNG), om binnen een jaar een campagne te starten naar de leden en de leveranciers om security.txt te implementeren, en om de leden ondersteuning te bieden bij de implementatie.

2. aan Rijksoverheidorganisaties om voortaan op hun domeinnamen te verwijzen naar de centrale security.txt die door NCSC wordt beheerd indien zij gebruik (willen) maken van het centrale CVD-beleid van de Rijksoverheid. NCSC heeft een Handreiking security.txt met uitleg gepubliceerd.
3. aan Shared Service Organizations (SSO) van de Rijksoverheid (zoals DPC, SSC-ICT, en DICTU) om te zorgen dat de domeinnamen die zij beheren, verwijzen naar de centrale door NCSC beheerde security.txt.
4. aan NCSC en DTC (indieners van de standaard) om security.txt voor langere termijn te promoten en ondersteuning te bieden aan overheidsorganisaties. Een van de middelen is het publiceren van een factsheet over inhoudelijke implementatie security.txt voor (semi) overheidsorganisaties, met daarin opgenomen de adviezen:
    - richt een CVD-beleid in.
    - host op een goed beheerde plek een centrale security.txt en laat individuele applicaties en sites van de organisatie middels HTTP(S) redirect (expliciet toegestaan in de standaard) doorverwijzen.
    - bij een gefaseerde implementatie is het inrichten van een security.txt op hoofddomeinen de eerste prioriteit.
    - security.txt kan niet worden gebruikt om eenzijdig voorwaarden op te leggen aan de melder van een kwetsbaarheid.
    - naast het up-to-date houden van security.txt (in het bijzonder de contactgegevens), dienen ook de contactgegevens in WHOIS, DNS (SOA) en andere plekken up-to-date gehouden te houden worden.
    - hoe aan te sluiten bij bestaande standaard tooling (zodat geautomatiseerde melders geen nieuwe standaarden hoeven te implementeren), wanneer voor het melden van een kwetsbaarheid in plaats van een e mailadres wordt verwezen naar een webformulier of API
5. aan NCSC en Logius om security.txt op te nemen in respectievelijk de eerstvolgende versie van de 'ICT-beveiligingsrichtlijnen voor webapplicaties' en eerstvolgende versie van het ‘DigiD Normenkader’.
6. aan Forum Standaardisatie om voortaan het gebruik van security.txt op domeinnamen van de overheid structureel te meten en daarover te rapporteren, in de marge van de IV-Metingen. De tool Internet.nl bevat de mogelijkheid voor meting van security.