Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

notitie

FORUM STANDAARDISATIE

Agendapunt:	FS-20170614.02A
Betreft:	Intake-advies voor STIX en TAXII
Aan:	Forum Standaardisatie
Van:	Stuurgroep open standaarden
Datum:	24 mei 2017

Advies

Het Forum Standaardisatie wordt geadviseerd om de informatiebeveiligingstandaarden STIX 1.2.1 en TAXII 1.1.1 in behandeling te nemen voor opname als verplichte standaard (pas-toe-of-leg-uit) op de lijst open standaarden. In procedure nemen van deze standaarden is van belang omdat deze standaarden het mogelijk maken om technische dreigingsinformatie breed en eenvoudig te delen tussen overheidsorganisaties. Dit verhoogt de digitale weerbaarheid van de overheid en instellingen in de (semi-) publieke sector. Opname op de lijst stimuleert de verdere adoptie van deze standaarden voor geautomatiseerd delen van dreigingsinformatie (binnen de overheid).

Korte toelichting:
De standaarden voldoen aan de criteria voor inbehandelname als verplichte standaard op de lijst open standaarden. De kansrijkheid van de procedure is voldoende. De standaard lost een bestaand en ervaren probleem op bij het delen van technische dreigingsinformatie. De standaard maakt gebruik van andere standaarden op de lijst, zoals XML, HTTPS en TLS maar dat is niet van invloed op de toetsing. De aanmelding van de standaard voor plaatsing op de lijst wordt expliciet ondersteund door de CTO-Raad Rijksoverheid, het RijksISAC en de IBD Gemeenten. De standaarden worden al gebruikt door het NCSC, de Belastingdienst, Rijkswaterstaat en SSC-ICT. De standaard heeft een duidelijke usecase binnen de (semi) publieke sector.

Toelichting

Datum
24 mei 2017

1. Aanmelding, intakegesprek en toetsingsprocedure

Op 28 april 2017 is door Arjan de Jong namens het Nationaal Cyber Security Centrum (NCSC) twee standaarden aangemeld, betreffende opname van STIX 1.2.1 en TAXII 1.1.1 op de lijst met open standaarden. De aanmelder heeft als doel de standaard verplicht ('pas-toe-of-leg-uit') te stellen.

Op 12 mei 2017 heeft een intakegesprek plaatsgevonden met de aanmelder. In dit gesprek is de aanmelding besproken. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure.

2. Korte beschrijving standaard

Waar gaan STIX en TAXII over?
STIX is een gestructureerde taal om technische dreigingsinformatie te beschrijven zodat het op een consistente manier kan worden gedeeld, opgeslagen en geanalyseerd. Via deze taal kunnen objecten zoals Incident, Indicator, Campaign en Course of Action worden beschreven. Technische dreigingsinformatie in het STIX-formaat kan geautomatiseerd verwerkt worden door onder andere beveiligingsapparatuur en –tooling. STIX 1.x maakt gebruik van XML als bestandsformaat.

TAXII is een transportmechanisme dat het geautomatiseerd uitwisselen van dreigingsinformatie standaardiseert. Het maakt gebruik van push/pull mechanismen op basis van abonnementen of kanalen en maakt voor het transport gebruik van HTTPS. TAXII kan worden gebruikt voor het uitwisselen van dreigingsinformatiedocumenten in STIX-formaat.

Welk probleem lost de standaard op?
Het NCSC streeft ter verhoging van de digitale weerbaarheid naar het zo breed en eenvoudig mogelijk delen van technische dreigingsinformatie. STIX en TAXII zijn standaarden om dit op een gestructureerde manier te doen. Het NCSC en een aantal andere partijen bij de rijksoverheid maken hier reeds gebruik van. Zonder deze standaard zouden partijen voor iedere koppeling separate afspraken moeten maken hoe gegevens uitgewisseld moeten worden. Het beschikbare alternatief OpenIOC biedt slechts voor een gedeelte een invulling.

Wie beheert de standaarden?
De standaarden worden beheerd door OASIS, een internationale standaardisatieorganisatie.

Waarom is de standaard aangemeld voor pas-toe-of-leg-uit?
Het geautomatiseerd delen van dreigingsinformatie (binnen de overheid) staat nog aan het begin, evenals de adoptie van standaarden voor uitwisseling. Het plaatsen van de STIX- en TAXII-standaarden op de lijst stimuleert het gebruik van deze standaarden en zal zo zorgen voor betere interoperabiliteit. Er ontstaat momentum voor de standaarden en opname op de lijst als verplichte standaarden kan dit momentum vergroten.

(zie ook: *7. Functionele use case*)

Datum
24 mei 2017

3. Criteria voor inbehandelname
Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijst. Hiervoor gelden drie criteria:

1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?
Ja, de standaard is toepasbaar bij elektronische gegevensuitwisseling van technische dreigingsinformatie tussen (semi-) overheidsorganisaties onderling of met bedrijven.

2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?
Ja, het uitwisselen en analyseren van technische dreigingsinformatie is van toepassing voor alle organisaties die de veiligheid van hun ICT-omgeving willen waarborgen. In de praktijk wordt de standaard gebruikt door bijvoorbeeld ICT Security Specialisten, Cyberdreiging Analisten, Malware Analisten, Security hard- en software producten, Security Operations Centers, Computer Emergency Response Teams en Security Onderzoekers.

3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?
Ja, er is geen wettelijk kader die het uitwisselen en analyseren van technische dreigingsinformatie regelt. Ook in de informatiebeveiligingsbaselines voor de overheid, zoals de Baseline Informatiebeveiliging Rijksdienst (BIR), zijn op dit vlak geen keuzes gemaakt.

4. Draagt de standaard bij aan de oplossing van een bestaand, relevant (interoperabiliteits)probleem en het voorkomen van leveranciersafhankelijkheid?
Ja, door de toename aan digitale dreigingen is er een grote behoefte aan interoperabele en efficiënte uitwisseling en verwerking van dreigingsinformatie. STIX en TAXII standaardiseren de uitwisseling van dreigingsinformatie. Doordat de standaard open is en door meerdere leveranciers wordt toegepast neemt de leveranciersafhankelijkheid af.

<u>Conclusie</u>
De standaard voldoet aan de criteria voor inbehandelname.

4. Toetsing kansrijkheid procedure
Het Forum Standaardisatie wil voorkomen dat er standaarden in procedure worden genomen, waarvan bij voorbaat al bekend is dat deze in de expertronde of consultatieronde zullen stranden op één van de inhoudelijke criteria. Daarom heeft de procedurebegeleider de beantwoording van de criteriavragen nagelopen, waar mogelijk zelf aangevuld en vervolgens besproken met de indiener.

1. Open standaardisatieproces
De ontwikkeling en het beheer van de standaard moeten op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.

STIX en TAXII worden beheerd door OASIS, een internationale onafhankelijke non-profit standaardisatieorganisatie, die de specificaties zonder belemmeringen beschikbaar stelt op haar website. Het intellectueel eigendomsrecht op de standaard stelt OASIS onherroepelijk royalty-free voor eenieder beschikbaar onder de OASIS Intellectual Property Rights Policy.

Het besluitvormingsproces van de standaard is toegankelijk voor iedereen die lid is van de OASIS Cyber Threat Intelligence Technical Committee. Iedereen kan lid worden. Het beheerproces voldoet ook overigens aan de eisen die het Forum stelt, zoals de mogelijkheid tot bezwaar, gepubliceerd beleid met betrekking tot versiebeheer en toegankelijke beheerdocumentatie.

De indiener raadt af het predicaat 'Uitstekend beheerproces' toe te kennen, doordat grote wijzigingen die doorgevoerd kunnen worden het wenselijk maken om aanvullende toetsing plaats te laten vinden.

2. Toegevoegde waarde
De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de kosten, de risico's en nadelen. Voor elk van de te onderscheiden stakeholders (overheid, bedrijven en burgers) afzonderlijk zouden de baten voor de informatievoorziening en de bedrijfsvoering op moeten wegen tegen de kosten. Verder moeten de risico's aan overheidsbrede adoptie van de standaard (beveiliging, privacy) acceptabel zijn.

Er is nog geen andere standaard die gaat over het uitwisselen van technische dreigingsinformatie. STIX en TAXII zijn de meest breed ondersteunde standaarden op dit gebied. Alleen OpenIOC is een standaard die voor een deel van het voorgestelde functionele toepassingsgebied een alternatief biedt. Om te voorkomen dat voor iedere koppeling uitgezocht moet worden hoe technische dreigingsinformatie kan worden uitgewisseld is het opnemen van deze standaard noodzakelijk. Door STIX en TAXII op te nemen op de lijst kan voorkomen worden dat vendor lock-in ontstaat door eigen formaten van leveranciers.

Met STIX en TAXII alleen is de interoperabiliteit nog niet gegarandeerd. STIX Profielen definiëren een subset van de STIX-objecten en attributen. Ze kunnen worden gebruikt om aan te geven dat slechts een subset van STIX wordt ondersteund of geproduceerd. Er is geen "de facto" STIX-profiel aan te wijzen. In beginsel staat een gebruiker de volledige STIX-standaard ter beschikking, maar als er een beperkt aandachtsgebied is of met een incomplete STIX-implementatie wordt gewerkt, kan het zinvol zijn dit te beschrijven in een STIX profiel. Het is denkbaar dat als STIX binnen de overheid meer gebruikt gaat worden er STIX-profielen worden opgesteld en op elkaar worden afgestemd. Het is nu echter te vroeg om al een STIX overheidsprofiel op te stellen en voor te schrijven. De indiener adviseert dan ook om STIX 1.2.1 zonder beperkend STIX-profiel als standaard op te nemen.

De beveiligingsrisico's aan de uitwisseling van dreigingsinformatie worden met deze standaard gemitigeerd door (tweezijdige) authenticatie en encryptie, door het gebruik van TLS. Privacyrisico's kunnen worden beheerst door een privacybeleid bijpassend bij de uitwisseling van dreigingsinformatie.

3. Draagvlak
Aanbieders en gebruikers moeten voldoende ervaring hebben met de implementatie en het gebruik van de standaard.

De standaarden STIX en TAXII zijn inmiddels in gebruik bij het NCSC, de Belastingdienst, Rijkswaterstaat en SSC-ICT. De standaarden STIX en TAXII worden ondersteund door Splunk, HP ArcSight, IBM QRadar en Alienvault. Ook is er open source tooling beschikbaar om een implementatie te valideren.

De standaard is relevant voor alle overheidsorganisaties (Rijk, provincies, gemeenten) en instellingen in de (semi-) publieke sector die in het kader van hun informatiebeveiliging technische dreigingsinformatie verzamelen en uitwisselen. Denk hierbij in het bijzonder aan Security Operations Centers. De CTO-Raad van de Rijksoverheid, het RijkISAC en de IBD Gemeenten ondersteunen expliciet de aanmelding van deze standaard bij het Forum Standaardisatie.

4. Opname bevordert adoptie
De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen.

Het geautomatiseerd delen van dreigingsinformatie (binnen de overheid) staat nog aan het begin, evenals de adoptie van standaarden voor deze gegevensuitwisseling. Het plaatsen van de STIX- en TAXII-standaarden op de lijst open standaarden stimuleert het gebruik van deze standaarden en zal zo zorgen voor betere interoperabiliteit. Er ontstaat momentum voor de standaarden en opname als verplichte standaard (pas-toe-of-leg-uit) op de lijst open standaarden kan dit momentum vergroten.

<u>Conclusie</u>
Er zijn op voorhand geen struikelblokken te verwachten.

5. Samenhang
Het Forum Standaardisatie wil weten of de aangemelde standaard samenhangt met standaarden die reeds op de lijst zijn opgenomen, of standaarden die voor toetsing in aanmerking komen. Uit de intake moet duidelijk worden of dit gevolgen heeft voor de toetsing en eventuele opname van de aangemelde standaard.

1. *Bestaat er samenhang tussen de aangemelde standaard en de verplichte ('pas-toe-of-leg-uit') standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*

   De standaard TAXII bouwt voort op https (TLS), IPv4/IPv6. Daarnaast is er samenhang met ISO 27001/27002, in de zin dat STIX en TAXII voor een aantal overheidsorganisaties invulling kan geven aan maatregelen die zij op basis van ISO 27001/27002 voor zichzelf gedefinieerd hebben. Dit heeft geen gevolgen voor de toetsing van STIX en TAXII.

2. *Bestaat er samenhang tussen de aangemelde standaard en de aanbevolen standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*

   De standaard TAXII bouwt voort op XML en URI. Dit heeft geen gevolgen voor de toetsing van STIX en TAXII.

3. *Bestaat er samenhang tussen de aangemelde standaard en standaarden die in aanmerking komen voor opname op de lijst en wat betekent dit voor de toetsing van de standaard(en)? (Denk bijvoorbeeld ook aan een gezamenlijke toetsing met (een deel van) deze aanvullende standaarden).*

   De standaarden STIX en TAXII bouwen voort op de andere standaarden, zoals (zover hierboven nog niet genoemd):
   - Common Attack Pattern Enumeration and Classification (CAPEC)
   - Common Event Expression (CEE)
   - Customer Information Quality (CIQ)
   - Common Platform Enumeration (CPE)
   - Common Vulnerabilities and Exposures (CVE)
   - Common Vulnerabilites Reporting Framework (CVRF)
   - Common Weakness Enumeration (CWE)
   - Date and time format – ISO 8601
   - Malware Attribute Enumeration and Characterization (MAEC)
   - OpenIOC
   - Open Vulnerability and Assessment Language (OVAL)
   - Documents associated with Unified Modeling Language (UML)
   - CybOX

   In de procedure zal tevens kort onderzoek verricht worden naar de mate waarin deze standaarden voldoen aan de criteria van het Forum Standaardisatie voor opneming op de lijst open standaarden.

6. Sponsorschap

De aanmelding van standaarden voor de lijst van het Forum en het Nationaal Beraad dient ondersteund of gesponsord te worden door overheids- en/of (semi)publieke organisaties die de standaard reeds in gebruik hebben (of voornemens zijn dit te doen) en die de beoogde opname op de lijsten ondersteunen. Dit draagt bij aan het draagvlak voor de standaard, geeft zicht op de functionele usecase voor de overheid en helpt bovendien om tijdens de toetsing de juiste experts te benaderen.

1. *Welke overheden en/of (semi)publieke organisaties ondersteunen de aanmelding van de standaard?*
   - CTO-Raad Rijksoverheid (SSC-ICT, RWS, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Belastingdienst, DICTU, Defensie Materiaal Organisatie, DJI, DUO, SSO-Noord, Nationale Politie, Logius, CIO-Rijk)
   - Rijks Information Sharing and Analysis Centre (RijksISAC) (Belastingdienst, Ministerie van Defensie, DICTU, Logius, Nationale Politie, NCSC, NZA, RWS, SSC-ICT, SVB, UWV, Ministerie van Veiligheid en Justitie, NBV, DJI SSC-I)
   - Informatiebeveiligingsdienst Gemeenten

2. Hebben deze organisaties de standaard geïmplementeerd?
   (zie ook punt 7 voor een uitwerking)
   Het NCSC streeft ter verhoging van de digitale weerbaarheid naar het zo breed en eenvoudig mogelijk delen van technische dreigingsinformatie. STIX en TAXII zijn standaarden om dit op een gestructureerde manier te doen. Het NCSC, de Belastingdienst, Rijkswaterstaat en SSC-ICT maken hier reeds gebruik van.

7. Functionele use case

Voor de standaard dient een duidelijke use case beschikbaar te zijn op basis waarvan overheden en/of instellingen uit de (semi) publieke sector kunnen bepalen of de aangemelde standaard voor hen relevant is en wie eventueel moet deelnemen aan de experttoetsing van de standaard.

Door het gebruik van STIX en TAXII kunnen het NCSC, de Belastingdienst, Rijkswaterstaat en SSC-ICT op een gestandaardiseerde manier dreigingsinformatie uit gaan wisselen. Zonder de standaarden STIX en TAXII hadden specifieke afspraken gemaakt moeten worden voor iedere koppeling tussen deze organisaties.