FS 20171011.3A

Forum Standaardisatie

Wilhelmina v Pruisenweg 104
2595 AN Den Haag
Postbus 84011
2508 AA Den Haag

www.forumstandaardisatie.nl

notitie

Opname STIX 1.2.1 en TAXII 1.1.1 op de 'pas toe of leg uit' lijst van open standaarden

FORUM STANDAARDISATIE 11 oktober 2017

Agendapunt:	FS 171011.3A
Bijlagen:	Expertadvies STIX 1.2.1 en TAXII 1.1.1-standaarden Overzicht reacties consultatieronde
Aan:	Forum Standaardisatie
Van:	Stuurgroep Standaardisatie
Datum:	19 september 2017

Aanleiding en achtergrond
Opname van deze standaarden is van belang omdat STIX 1.2.1 en TAXII 1.1.1 het mogelijk maken om gestructureerde dreigingsinformatie over digitale dreigingen tegen informatiesystemen 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).

Betrokkenen en proces
De standaard is aangemeld door het NCSC op 28 april 2017. Door het Bureau Forum Standaardisatie is een intakegesprek gevoerd met de indiener van de standaarden STIX 1.2.1 en TAXII 1.1.1. Tijdens de intake zijn de standaarden getoetst op uitsluitingscriteria en is een eerste inschatting gemaakt van de kansrijkheid van de procedure. Naar aanleiding daarvan heeft het Forum Standaardisatie besloten de standaarden in procedure te nemen. Op basis van dit besluit is de expertgroep op 4 juli 2017 bijeengekomen om de standaard, de aandachtspunten en openstaande vragen uit het voorbereidingsdossier te bespreken. Tijdens deze bijeenkomst is ook het advies ten aanzien van het functioneel toepassingsgebied vastgesteld. Het expertadvies is beschikbaar gesteld voor publieke consultatie. Dit heeft één reactie opgeleverd.

Consequenties en vervolgstappen
Er zijn geen specifieke risico's verbonden aan het besluit. Het Forum Standaardisatie zal op basis van het Forumadvies en de relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad bepaalt uiteindelijk op basis van het advies of STIX 1.2.1 en TAXII 1.1.1 op de lijst open standaarden wordt opgenomen met als status 'pas toe of leg uit'.

Gevraagd besluit

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaand advies:

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om:
1. de standaarden STIX 1.2.1 en TAXII 1.1.1 op te nemen op de 'pas toe of leg uit'-lijst
2. betrokken partijen op te roepen tot uitvoering van de adoptieadviezen ten aanzien van STIX 1.2.1. en TAXII 1.1.1.

Ad 1
Als functioneel toepassingsgebied wordt geadviseerd:
STIX 1.2.1 en TAXII 1.1.1 moeten worden toegepast op de gestructureerde uitwisseling van informatie over digitale dreigingen tegen informatiesystemen.

Als organisatorisch werkingsgebied wordt geadviseerd:
Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

Ad 2 Additionele adviezen ten aanzien van de adoptie van de standaard
Ten aanzien van de adoptie van STIX 1.2.1 en TAXII 1.1.1 adviseert de expertgroep de volgende oproepen te doen:
1. Het Forum roept het NCSC op om samen met betrokkenen een leidraad op te stellen, al dan niet als onderdeel van een bestaand kennisproduct, ten behoeve van het eenduidig gebruik van de standaarden. De toepassing van STIX en TAXII zal veel effectiever zijn als ook op het vlak van semantiek standaardisatie plaatsvindt. De leidraad moet dit borgen. Onderdeel van de leidraad dient ook te zijn dat bij het gebruik van STIX en TAXII de toepassing van CybOx wordt geadviseerd.
2. Het Forum adviseert het NCSC om mede in de context van het Nationaal Detectie Netwerk (een samenwerking van onder andere het NCSC voor het beter en sneller waarnemen van digitale gevaren en risico's) kennisbijeenkomsten te organiseren voor het verspreiden van kennis over en ervaring met het gebruik van STIX en TAXII.
3. Het Forum roept betrokkenen bij SOC's (security operations centres) en CERT's (computer emergency response teams) binnen de overheid en publieke sector op om kennis op te doen over de meerwaarde en toepassing van de uitwisseling van gestructureerde dreigingsinformatie met STIX en TAXII.
4. Het Forum roept overheden die STIX en TAXII toepassen op om informatie over de meerwaarde van het gebruik voor hen en best practices te delen.
5. Het Forum roept KING op om in de GGI (gemeentelijke gemeenschappelijke infrastructuur) STIX en TAXII toe te passen in het SOC (security operations center).

De expertgroep adviseert het Forum Standaardisatie de adoptie en deze oproepen na 2 jaar te evalueren.

Toelichting

1. Waar gaat het inhoudelijk over?
STIX is een gestructureerde taal om 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. Gestructureerde 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.

2. Hoe is het proces verlopen?
De standaard is aangemeld door het NCSC op 28 april 2017. Door het Bureau Forum Standaardisatie is een intakegesprek gevoerd met de indiener van de standaarden STIX 1.2.1 en TAXII 1.1.1. Tijdens de intake zijn de standaarden getoetst op uitsluitingscriteria en is een eerste inschatting gemaakt van de kansrijkheid van de procedure. Naar aanleiding daarvan heeft het Forum Standaardisatie besloten de standaarden in procedure te nemen. Op basis van dit besluit is de expertgroep op 4 juli 2017 bijeengekomen om de standaard, de aandachtspunten en openstaande vragen uit het voorbereidingsdossier te bespreken. Tijdens deze bijeenkomst is ook het advies ten aanzien van het functioneel toepassingsgebied vastgesteld. Het expertadvies is beschikbaar gesteld voor publieke consultatie. Dit heeft één reactie opgeleverd.

3. Hoe scoort de standaard op de toetsingscriteria?

Open standaardisatieproces
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 is om aanvullende toetsing plaats te laten vinden.

Toegevoegde waarde
Er is nog geen andere standaard die gaat over het uitwisselen van gestructureerde dreigingsinformatie. STIX 1.2.1 en TAXII 1.1.1 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 gestructureerde dreigingsinformatie kan worden uitgewisseld is het opnemen van deze standaard noodzakelijk. Door STIX 1.2.1 en TAXII 1.1.1 op te nemen op de lijst kan

voorkomen worden dat vendor lock-in ontstaat door eigen formaten van leveranciers.

Met STIX 1.2.1 en TAXII 1.1.1 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.

Draagvlak
De standaarden STIX 1.2.1 en TAXII 1.1.1 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, Alienvault, EclecticIQ, ThreatConnect, Anomali en ThreatQuotient. 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 gestructureerde dreigingsinformatie verzamelen en uitwisselen. Denk hierbij in het bijzonder aan Security Operations Centers. De CTO-Raad van de Rijksoverheid, het RijksISAC en de nformatiebeveiligingsdienst voor gemeenten (IBD) ondersteunen expliciet de aanmelding van deze standaard bij het Forum Standaardisatie.

Opname bevordert de 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.

Toelichting van eventuele risico's
Door de expertgroep zijn de volgende aandachtspunten onderschreven:
- De beveiligingsrisico's aan de uitwisseling van dreigingsinformatie worden met deze standaard gemitigeerd door (tweezijdige) authenticatie en encryptie, door het gebruik van TLS.
- De privacygevoelige informatie die met STIX en TAXII kan worden uitgewisseld betreft doorgaans informatie over aanvallers van digitale omgevingen. De daaraan verbonden privacyrisico's wegen over het algemeen op tegen het doel van het delen van deze informatie: het verhogen van de digitale weerbaarheid van de (semi-) overheidsorganisaties. Privacyrisico's kunnen worden beheerst door een privacybeleid bijpassend bij de uitwisseling van dreigingsinformatie.
- Het is de verantwoordelijkheid van de gebruikers van STIX en TAXII om bij het uitwisselen van informatie de geldende privacyregelgeving te hanteren en een eigen afweging te maken van de privacyrisico's.

4. Wat is de conclusie van de expertgroep en de consultatie?

Conclusie van de expertgroep
De experts adviseren het Forum Standaardisatie de standaarden STIX en TAXII op te nemen op de lijst open standaarden met de status 'pas toe of leg uit'.

Eventuele aanvullingen vanuit de consultatie
Op de openbare consultatie van het expertadvies is één reactie ontvangen (van Gemeente Zevenaar). In de reactie wordt opgemerkt dat:
- de impact van de 'pas toe of leg uit'-verplichting voor gemeenten onduidelijk is, ondanks de bijdrage aan het expertadvies door IBD,
- een standpunt van KING/VNG wordt gemist,
- onduidelijk is op welke wijze de standaard toegepast moet worden, zodat voldaan kan worden aan de 'pas toe of leg uit'-verplichting, en
- onduidelijk is welke GEMMA-component relevant is.

5. Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?

Ten aanzien van de adoptie van STIX 1.2.1 en TAXII 1.1.1 adviseert de expertgroep de volgende oproepen te doen:
1. Het Forum roept het NCSC op om samen met betrokkenen een leidraad op te stellen, al dan niet als onderdeel van een bestaand kennisproduct, ten behoeve van het eenduidig gebruik van de standaarden. De toepassing van STIX en TAXII zal veel effectiever zijn als ook op het vlak van semantiek standaardisatie plaatsvindt. De leidraad moet dit borgen. Onderdeel van de leidraad dient ook te zijn dat bij het gebruik van STIX en TAXII de toepassing van CybOx wordt geadviseerd.
2. Het Forum adviseert het NCSC om mede in de context van het Nationaal Detectie Netwerk (een samenwerking van onder andere het NCSC voor het beter en sneller waarnemen van digitale gevaren en risico's) kennisbijeenkomsten te organiseren voor het verspreiden van kennis over en ervaring met het gebruik van STIX en TAXII.
3. Het Forum roept betrokkenen bij SOC's (security operations centres) en CERT's (computer emergency response teams) binnen de overheid en publieke sector op om kennis op te doen over de meerwaarde en toepassing van de uitwisseling van gestructureerde dreigingsinformatie met STIX en TAXII.
4. Het Forum roept overheden die STIX en TAXII toepassen op om informatie over de meerwaarde van het gebruik voor hen en best practices te delen.
5. Het Forum roept KING op om in de GGI (gemeentelijke gemeenschappelijke infrastructuur) STIX en TAXII toe te passen in het SOC (security operations center).

De expertgroep adviseert het Forum Standaardisatie de adoptie en deze oproepen na twee jaar te evalueren. De opgeroepen partijen worden gevraagd om op deze termijn (na opname van de standaard) over de voortgang op deze punten te rapporteren aan het Forum Standaardisatie.

Bijlagen
- Expertadvies voor opname STIX 1.2.1 en TAXII 1.1.1 op de 'pas toe of leg uit'-lijst
- Overzicht reacties consultatieronde