Gespreksnotitie regierol standaarden STIX TAXII in Nederland

Aan:	NCSC
Van:	Bureau Forum Standaardisatie
Datum:	Vrijdag 23 december 2022
Onderwerp:	Regierol op STIX en TAXII (standaarden voor cyberdreigingsinformatie) in Nederland
Type:	Ter bespreking

Inleiding

Deze notitie adresseert het ontbreken van de sturende rol (regierol) in Nederland op de open standaarden STIX en TAXII (standaarden voor cyberdreigingsinformatie) en stelt voor het gesprek hierover te starten met het NCSC. Het ontbreken van de regierol is de hoofduitkomst van het Evaluatierapport Veilig Internet (2022) in opdracht van Forum Standaardisatie waarin de open standaarden STIX en TAXII zijn geëvalueerd.

STIX en TAXII (cyberdreigingsinformatie) dragen bij aan een veiliger internet doordat cyberdreigingsinformatie gemakkelijker en sneller wordt uitgewisseld. De standaarden zijn verplicht voor de overheid ('pas toe of leg uit'-verplichting) en staan op de Lijst Verplichte Standaarden van het Forum Standaardisatie.

Voorstel Forum Standaardisatie

Het Forum Standaardisatie adviseert een regierol vanuit de Nederlandse overheid op STIX en TAXII. Forum Standaardisatie stelt voor een gesprek op te starten met NCSC over het nemen van de regierol door NCSC voor het stimuleren van adoptie van STIX en TAXII en voor het zijn van aanspreekpunt voor Nederlandse overheden voor deze standaarden. NCSC heeft STIX en TAXII op 28 april 2017 aangemeld voor de Lijst Verplichte Standaarden. NCSC werkt als expert aan een veilig digitaal Nederland en is de verbindende partij voor veilig digitaal Nederland.

Regierol STIX en TAXII Nederlandse overheid

In Nederland ontbreekt een regierol vanuit de Nederlandse overheid op STIX en TAXII. Uitwisseling van dreigingsinformatie is belangrijk. De open standaarden STIX en TAXII dragen hieraan bij.

Cybersecurity wordt in belangrijke mate vanuit het perspectief van de dreiging (en dus in termen van risico's) beleefd (Nederlandse Cybersecuritystrategie 2022-2028). Het is te verwachten dat de Nederlandse overheid een sturende rol (regierol) wil hebben op standaarden over dreigingsinformatie. Deze regierol draagt bij aan het vergroten van de digitale weerbaarheid door grip te houden op het beheerproces en op de adoptie van STIX en TAXII. Regierol zorgt ervoor dat Nederlandse overheden aansluiten bij internationale ontwikkelingen rond STIX en TAXII en rond melden van dreigingsinformatie in het algemeen.

Regierol kan bestaan uit stimuleren van adoptie van de standaarden bij overheden. Het Bureau Forum Standaardisatie heeft vanuit het veld signaal ontvangen dat er de behoefte is aan ondersteuning, zoals in de vorm van documentatie.

Daarnaast is het van belang aansluiting te zoeken bij internationale ontwikkelingen over STIX en TAXII. Internationale uitwisseling van kennis verhoogt het kennisniveau over STIX en TAXII. STIX en TAXII zijn internationale standaarden. Overheden in andere landen, waaronder Groot Brittannië en de Verenigde Staten, zijn betrokken bij internationale beheerorganisatie OASIS en zij ontwikkelen nationale profielen op de standaarden.

Aansluiting bij de beheerorganisatie OASIS draagt bij aan grip en zicht op het beheerproces waardoor de Nederlandse overheid op de hoogte is van de meest recente ontwikkelingen rond STIX en TAXII.

STIX en TAXII: verweesde standaarden in Nederland

Uit het Evaluatierapport Veilig Internet is naar voren gekomen dat STIX en TAXII in Nederland verweesde standaarden zijn. Verweesde standaarden zijn standaarden die wel op de Lijst Open Standaarden van Forum Standaardisatie staan, maar geen partij hebben die regierol voert voor adoptie en/ of voor (doorontwikkeling i.s.m.) de (inter)nationale beheerorganisatie. Er is in de Nederlandse overheid geen partij die internationaal is betrokken bij de ontwikkeling van nieuwe versies van de standaard. Daarnaast is er op dit moment geen inspanning om nieuwe versies van de standaarden te monitoren en aan te melden bij Lijst Open Standaarden

Evaluatie STIX en TAXII (veilig internet)

STIX en TAXII zijn in het najaar 2022 geëvalueerd. De evaluatie is gepubliceerd in het Evaluatierapport Veilig Internet. In het rapport staat een aantal aanbevelingen die het Forum Standaardisatie heeft overgenomen (zie bijlage). Voor de evaluatie is gesproken met experts

(beheerorganisatie, gebruikers van de standaard en leveranciers van software die de standaarden implementeren), waaronder NCSC, SSC-ICT, IBD, SURF en Agentschap Telecom.

Het Forum Standaardisatie evalueert jaarlijks een aantal standaarden op de 'Pas toe of leg uit'-lijst. Het doel van dit onderzoek is om de kwaliteit van de informatie op de lijst te waarborgen. Het onderzoek richt zich met name op de huidige relevantie van de standaard, het functioneel toepassingsgebied, het beheer en de stand van zaken rond de adoptie van de standaard.

Bijlage:

Aanbevelingen uit Evaluatierapport Veilig Internet

Hieronder volgen de belangrijkste aanbevelingen uit het Evaluatierapport Veilig Internet:

1. In gesprek gaan met het NCSC over de regierol op STIX en TAXII gezien het NCSC de aanmelder van de standaarden op de 'pas toe of leg uit'-lijst is geweest.

2. In samenwerking met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties afdeling Digitale Samenleving onderzoeken waar de regierol voor Nederland voor STIX en TAXII binnen de Nederlandse overheid het beste is belegd en hierover adviseren.

3. Tussen de twee en vier jaar de standaarden opnieuw te evalueren. De markt rondom cyberdreigingsinformatie groeit en is in beweging. De kans dat er op een middellange termijn ontwikkelingen zijn die de standaarden raken is groot.

Zodra de regierol voor STIX en TAXII voor Nederland belegd is binnen de Nederlandse overheid, zijn de volgende aanbevelingen gericht aan de partij die de regierol op zich neemt:

4. Contact leggen met partijen die actief zijn in STIX- en TAXII-committee bij de beheerorganisatie OASIS met als doel om zicht en grip te krijgen op het beheerproces en op internationale ontwikkelingen.

5. Opnieuw onderzoeken van het nut en de noodzaak van de adoptieadviezen. De experts geven geen signalen dat er behoefte is aan kennisdeling over de standaard. Daarentegen loopt de adoptie bij gemeenten en waterschappen achter en is de potentiële meerwaarde van de standaard niet helder voor alle organisaties.

6. Uitdragen en communiceren van toegevoegde waarde van STIX en TAXII.

7. Onderzoeken in hoeverre er sprake is bij STIX en TAXII van leveranciersafhankelijkheid door de sterke rol van leveranciers in de ontwikkeling en in het uitdragen van de standaard.