Intakeadvies SBOM

Vergadering:	Forum Standaardisatie 25 juni 2025
Agendapunt:	04C
Documentnummer:	04C
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	6 juni 2025
Versie:	1.0
Bijlagen:	geen
Rechten:	CC0 publieke domein verklaring

1 Samenvatting en advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om de aangemelde standaarden CycloneDX en SPDX onder de noemer SBOM voor nu niet in procedure te nemen zolang Europese harmonisatie nog gaande is.

Een Software Bill of Materials (SBOM) is een document dat alle componenten, bibliotheken en frameworks beschrijft waaruit een softwareproduct bestaat. Dit geldt voor zowel open als closed source softwareproducten. De indiener heeft voor de invulling van een SBOM twee open standaarden aangemeld: CycloneDX versie 1.5 en Software Package Data Exchange (SPDX) versie 3.0. Beide worden internationaal ondersteund en zijn technisch volwassen. De standaarden hebben onderling wel een overlappende functionaliteit.

De Europese Unie ontwikkelt via de Cyber Resilience Act (CRA) en bijbehorende standaardisatieverzoeken geharmoniseerde eisen voor Software Bills of Materials (SBOMs). De CRA, die 10 december 2024 officieel in werking trad, verplicht via bijlage I, sectie 2 fabrikanten om SBOMs bij hun producten te leveren in een machineleesbaar formaat. De Europese Commissie heeft in februari 2025 een standaardisatieverzoek ingediend bij CEN, CENELEC en ETSI voor het ontwikkelen van technische specificaties, ook voor onderwerpen rond SBOMs, zoals minimale set elementen, formaat en beheerprocessen. Het verplichten (‘Pas toe of leg uit’) of het aanbevelen van een specifieke SBOM-standaard brengt het risico

met zich mee dat de EU op termijn een andere standaard voorschrijft dan die in Nederland door het Forum Standaardisatie reeds wordt verplicht (‘Pas toe of leg uit’) of aanbevolen. Dit kan leiden tot dubbele implementatiekosten en belemmerde interoperabiliteit.

SBOMs zijn bedoeld om inzicht te geven in de samenstelling van softwareproducten en daarmee risico’s in de softwareketen beter beheersbaar te maken. Daarmee kunnen SBOMs bijdragen aan sneller en gerichter reageren op kwetsbaarheden. In de praktijk blijkt de toegevoegde waarde echter nog beperkt. Doordat gangbare standaarden zoals SPDX en CycloneDX vrijwel alle velden optioneel maken, kunnen SBOMs formeel correct zijn, maar inhoudelijk nagenoeg leeg of onbruikbaar. Bijvoorbeeld: een SBOM kan enkel met licentie-informatie gevuld zijn of zonder concrete componentgegevens. Zonder duidelijke minimumeisen of profielen is het lastig om SBOMs betrouwbaar in te zetten voor beveiliging, compliance of risicobeoordeling,

Gezien de huidige situatie is het advies:

- Aan de indiener en Forum Standaardisatie om het Europese standaardisatieproces voor SBOM-standaarden actief te monitoren. Heroverweeg het intakeadvies zodra geharmoniseerde EU-normen beschikbaar komen. Tot die tijd moet het Forum Standaardisatie terughoudend zijn met het adviseren tot verplichten (‘Pas toe of leg uit’) of aanbevelen van een specifieke SBOM-standaard.
- Betrokken partijen zoals het Nationaal Cyber Security Centrum (NCSC), het Ministerie van Economische Zaken en het Nederlands Normalisatie Instituut (NEN) zouden niet alleen een volgende rol moeten hebben, maar ook een actieve rol kunnen pakken in het behartigen van de Nederlandse belangen binnen de Europese normontwikkeling. Door vroegtijdige en inhoudelijke betrokkenheid kunnen Nederlandse praktijkervaringen worden ingebracht in het Europese proces. Het is van belang dat deze partijen actief deelnemen aan werkgroepen, consultaties en afstemmingsoverleggen binnen de Europese normalisatie-instellingen om zo invloed uit te kunnen oefenen op de totstandkoming van werkbare en toepasbare normen.

In de rest van dit document wordt het advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. In Hoofdstuk 4 worden de resultaten van de toetsing beschreven of de standaarden voldoen aan de criteria om in behandeling genomen te worden door het Forum Standaardisatie. In hoofdstuk 5 wordt vooruitgeblikt op een toetsing van de standaarden aan de hand van de inhoudelijke criteria. Tot slot worden er in hoofdstuk 6 praktijkvoorbeelden gegeven van het gebruik van SBOM-standaarden door derde organisaties.

2 Korte beschrijving van de standaard

2.1 Over de standaard

De standaarden CycloneDX en SPDX zijn beide SBOM-standaarden. Een SBOM is een document dat alle onderdelen (componenten, bibliotheken en frameworks) beschrijft waaruit een softwareproduct bestaat. Alle softwareproducten (open en closed source) zijn opgebouwd uit een of meerdere componenten. In de meeste gevallen worden daarvoor open source componenten gebruikt.

Op dit moment zijn CycloneDX en SPDX de veelgebruikte standaarden om een SBOM te beschrijven. Beide standaarden specificeren de manier waarop softwarecomponenten, licenties, versies en relaties in een softwareproduct vastgelegd kunnen worden. Hierdoor is integratie en uitwisseling tussen verschillende systemen eenvoudiger en wordt het beheer van het softwarelandschap verbeterd.

2.2 Waarom is deze standaard belangrijk?

Als SBOM-standaarden bieden CycloneDX en SPDX inzicht in de samenstelling van een softwareproduct, wat bijdraagt aan transparantie, hergebruik, veiligheid en beheer van deze producten. Het stelt organisaties in staat om naleving van licenties en regelgeving beter te waarborgen, mogelijk hergebruik van componenten te beoordelen, afhankelijkheden in kaart te brengen en sneller te reageren op veiligheidsincidenten rond componenten. Het komt namelijk regelmatig voor dat er meer of minder ernstige kwetsbaarheden worden gevonden in componenten. Dat kan als gevolg hebben dat softwareproducten waarin zo'n component wordt gebruikt zelf ook kwetsbaar zijn. Alle softwareproducten waar het component in wordt gebruikt moeten worden geïdentificeerd zodat passende maatregelen kunnen worden genomen. CycloneDX en SPDX versnellen dit proces met het geboden inzicht. En wanneer ze in een doorzoekbaar register beschikbaar zijn, dan is het bij het bekend worden van een kwetsbaarheid nog makkelijker om de geraakte softwarecomponent te achterhalen. Dit hoeft dan niet eerst geïnventariseerd te worden.

De Wet hergebruik van overheidsinformatie (Who) verplicht instellingen met een publieke taak om overheidsinformatie beschikbaar te stellen op een manier die openheid en hergebruik ervan faciliteert en vergemakkelijkt. Om dit met de juiste zorgvuldigheid vorm te geven is het nodig inzicht te hebben in de componenten waaruit het softwareproduct is opgebouwd. Van elk van de componenten moet worden gecontroleerd onder welke licenties ze zijn vrijgegeven. Met een SBOM wordt het eenvoudiger om inzicht te krijgen in de componenten waaruit een softwareproduct is opgebouwd.

Toepassing van een SBOM-standaard kan met het geboden inzicht ook het vertrouwen in het softwarelandschap versterken, wat belangrijk is in een tijd waarin software steeds vaker afhankelijk is van open source componenten en componenten van derden.

Voor het daadwerkelijk hergebruik van overheidssoftwareproducten helpt het wanneer anderen kunnen zien uit welke componenten deze zijn opgebouwd. Met het geboden inzicht

van SBOM-standaarden kan bepaald worden of de software en/of de componenten compliant zijn met daarvoor vastgestelde regels. Dit maakt het voor derden makkelijker om de herbruikbaarheidswaarde van door de overheid ontwikkelde software te bepalen. Datzelfde geldt ook bij het gebruik van open source software en/of componenten. Ook voor de overheid wordt het makkelijker om deze aan de eigen compliance regels te toetsen.

3 Betrokkenen en proces

Op 25 juni 2024 heeft Maurice Hendriks (Ministerie van Volksgezondheid, Welzijn en Sport (VWS), mede namens Karel Rietveld (Belastingdienst) en Leon C. Roeleveld (UWV) de SBOM-standaarden CycloneDX versie 1.5 en SPDX versie 3.0 onder de noemer SBOM aangemeld voor opname op de 'Pas toe of leg uit'-lijst of de lijst aanbevolen standaarden.

Op 7 november 2024 heeft een intakegesprek plaatsgevonden met de indiener, procedurebegeleider InnoValor Advies en Bureau Forum Standaardisatie. Bij het online intakegesprek waren de volgende personen aanwezig:

- Maurice Hendriks (Ministerie van Volksgezondheid, Welzijn en Sport (VWS) - indiener
- Aday Destici (InnoValor Advies)
- Ruud Kosman (InnoValor Advies)
- Benjamin Broersma (Bureau Forum Standaardisatie)
- Wouter Kobes (Bureau Forum Standaardisatie)
- Joram Verspaget (Bureau Forum Standaardisatie)

In dit gesprek is verkend of SBOM voldoet aan de criteria om in procedure genomen te worden. Daarnaast is vooruitgeblikt op de toetsingsprocedure. Dit intakeadvies is tot stand gekomen op basis van de informatie in het aanmeldformulier en aanvullende informatie uit het intakegesprek. Aanvullend hierop zijn gesprekken gevoerd door Bureau Forum Standaardisatie met de indiener en het Ministerie van Economische Zaken.

4 Voldoet de standaard aan de criteria om in procedure genomen te worden?

In het intakeonderzoek is vastgesteld dat de standaarden CycloneDX en SPDX niet voldoen aan alle vier criteria om in behandeling genomen te worden voor plaatsing op de 'Pas toe of leg uit' lijst. Dit wordt toegelicht in paragrafen 4.1 tot en met 4.4.

4.1 Is de standaard toepasbaar op elektronische gegevens-uitwisseling tussen en met (semi)overheidsorganisaties?

CycloneDX en SPDX zijn toepasbaar op elektronische gegevensuitwisseling tussen en met (semi)overheidsorganisaties, mits er duidelijkheid is over de te hanteren standaard. SBOM is als principe geen standaard op zichzelf, maar er bestaan wel verschillende open standaarden, zoals SPDX en CycloneDX, die hiervoor worden gebruikt.

Voor effectieve en betrouwbare gegevensuitwisseling is het cruciaal dat (semi)overheden gezamenlijk kiezen voor één gestandaardiseerde manier van vastleggen en delen. Dit maakt consistente, transparante en veilige communicatie over softwarecomponenten mogelijk en ondersteunt de interoperabiliteit binnen het publieke domein.

4.2 Draagt de standaard bij aan de interoperabiliteit van de (semi)overheid voor de desbetreffende functionaliteit?

Het gebruik van SBOM-standaarden als CycloneDX en SPDX draagt bij aan verbeterde interoperabiliteit binnen het publieke domein. Een SBOM biedt gedetailleerd inzicht in de samenstelling van zowel ingekochte als zelf ontwikkelde softwareproducten. Hierdoor kan de overheid beter toetsen of software voldoet aan de gestelde (niet-)functionele eisen, gerichter sturen op de opbouw van de softwareportfolio en sneller reageren op kwetsbaarheden.

Doordat een SBOM gestandaardiseerde en gedetailleerde informatie biedt over gebruikte softwarecomponenten, licenties, versies en kwetsbaarheden binnen het gehele ICT-portfolio, kunnen (semi)overheidsorganisaties en hun partners eenvoudig en eenduidig deze gegevens uitwisselen. Het gebruik van SBOM-standaarden als SPDX en CycloneDX maakt deze informatie breed en eenduidig toepasbaar en bevordert consistente samenwerking tussen systemen.

4.3 Is de standaard niet al wettelijk verplicht?

Het gebruik van de standaarden CycloneDX en SPDX is niet wettelijk verplicht. De Cyber Resilience Act (CRA) - die rechtstreeks van toepassing is op alle EU-lidstaten – kan echter wel kan invloed zijn op welke SBOM-standaarden te gebruiken.

Vooralsnog schrijft de CRA geen specifieke SBOM-standaarden voor. De CRA en de standardisation request M/606 van de Europese Commissie geeft wel aan dat er stappen worden gezet richting standaardisatie in het kader van cybersecurity. Daarnaast is er recent een *call for tender* gepubliceerd voor het STAN4CR2-project (joint working group). Dit project ondersteunt en versnelt EU-standaardisatie-inspanningen op het gebied van cybersecurity, met als doel samenwerking te bevorderen om beveiligingsincidenten te voorkomen. Met het project werkt de EU via CEN, CENELEC en ETSI aan geharmoniseerde standaarden.

Het verplichten (‘Pas toe of leg uit’) of het aanbevelen van een specifieke SBOM-standaard brengt het risico met zich mee dat de EU op termijn een andere standaard voorschrijft dan die in Nederland door het Forum Standaardisatie reeds wordt verplicht (‘Pas toe of leg uit’) of aanbevolen. Dit kan leiden tot dubbele implementatiekosten en belemmerde interoperabiliteit.

4.4 Draagt de standaard bij tot de oplossing van een bestaand probleem?

Een SBOM-standaard draagt in principe bij aan de oplossing van een bestaand probleem, namelijk het gebrek aan inzicht in de samenstelling van softwarecomponenten. SBOMs zijn

bedoeld om transparantie te creëren over welke softwarebibliotheken en afhankelijkheden in een applicatie worden gebruikt – inclusief eventuele kwetsbaarheden.

In hun huidige vorm dragen het verplichten ('Pas toe of leg uit') of het aanbevelen van CycloneDX en SPDX echter niet bij aan de oplossing van bestaande problemen. Dit komt door een aantal beperkingen:

Hoewel er meerdere SBOM-standaarden bestaan, zoals SPDX en CycloneDX, ontbreekt het aan één algemeen geaccepteerde, universele standaard. Dit kan leiden tot versnippering en kan het voor overheidsorganisaties lastig maken om eenduidig informatie over de samenstelling van digitale producten uit te wisselen en te integreren in hun processen.

Zelfs bij gebruik van bestaande standaarden ontbreekt een vastgelegd profiel dat voorschrijft hoe deze moeten worden toegepast. Verschillen in detailniveau, updatefrequentie en opgenomen metadata zorgen voor inconsistenties die de praktische bruikbaarheid en interoperabiliteit belemmeren.

Ook ontbreekt een al dan niet voorgeschreven gangbare standaard met een eenduidig toepassingsprofiel. Dit bemoeilijkt de inzet van SBOMs in de praktijk en roept vragen op zoals: welke standaard moet ik kiezen, hoe gedetailleerd moet deze zijn, en hoe verwerk ik de informatie in mijn bestaande processen?

Een voorbeeld van een mogelijke oplossing is het Duitse model. De Duitse overheid ontwikkelde een specifiek profiel op CycloneDX, zoals beschreven in de technische richtlijn TR-03183 van het Bundesamt für Sicherheit in der Informationstechnik (BSI). Dit profiel legt een vaste structuur op aan een SBOM-standaard, met gedefinieerde eisen en verplichte velden, wat zorgt voor een consistentere en effectievere toepassing.

Ten slotte geven de ontwikkelingen op EU-niveau, zoals beschreven in paragraaf 4.3, aan dat bredere standaardisatie in de toekomst mogelijk de noodzaak voor nationale maatregelen zal verminderen.

5 Is er zicht op een positief expertadvies?

Op basis van de eerder beschreven en gewogen ontwikkelingen is het advies om de aangemelde standaarden op dit moment niet in behandeling te nemen. Er is nu geen zicht op een positief expertadvies.

Toch zijn er wel concrete positieve aanknopingspunten voor een eventuele latere aanmelding van deze en/of andere SBOM-standaarden. SBOM-standaarden als CycloneDX en SPDX hebben een duidelijke meerwaarde en de ontwikkelingen vauit Europa onderschrijven het belang van de adoptie van SBOMs.

Wel zijn er meerdere aandachtspunten voor verder onderzoek in een eventuele latere toetsingsprocedure:

- De mogelijke overlappende functionaliteit tussen CycloneDX en SPDX, die nader onderzocht moet worden.

- Het belang van het beleggen van een regierol voor beide standaarden bij een geschikte nationale organisatie, om de adoptie in Nederland te stimuleren en Nederlandse belangen te vertegenwoordigen bij de verdere ontwikkeling van de standaarden.

Ondanks het advies om SPDX en ClycloneDX niet in procedure te nemen, wordt in dit intakeadvies vooruitgeblikt op de vier inhoudelijke criteria voor een eventuele latere aanmelding van deze en/of andere SBOM-standaarden. Dit wordt toegelicht in paragrafen 5.1-5.4.

5.1 Toegevoegde waarde

De toegevoegde waarde van een SBOM ligt in het vergroten van transparantie en controle over het softwarelandschap van de overheid. Een SBOM biedt inzicht in het softwareproduct dat aan de overheid wordt aangeboden, zodat gecontroleerd kan worden of deze voldoet aan de (niet-)functionele eisen. Daarnaast geeft het inzicht in het ingekochte softwareproduct, wat organisaties in staat stelt om effectiever softwarekwetsbaarheden in kaart te brengen en hierop te acteren. Ook wordt sturingsinformatie gegenereerd over de aard en opbouw van het softwareportfolio, wat helpt bij strategische besluitvorming en risicoanalyse. Tot slot biedt een SBOM inzicht in de opbouw van door de overheid zelf ontwikkelde softwareproducten, wat bijdraagt aan betere beheerbaarheid en naleving van veiligheids- en interoperabiliteitseisen.

SBOM-standaarden als SPDX en CycloneDX conflicteren niet met bestaande gegevensuitwisselingsstandaarden. Integendeel, ze bouwen hierop voort door gebruik te maken van al aanbevolen formaten zoals JSON en XML. Er zijn nog geen concrete kosten voor de implementatie van de standaard inzichtelijk. Om een SBOM in te zetten als een overheidsbreed sturingsinstrument, kan het ontwikkelen van een doorzoekbaar SBOM-register worden overwogen. Daarmee kan het eenvoudiger worden om structureel inzicht te krijgen in gebruikte softwarecomponenten. Het is aannemelijk dat dit register zowel eenmalige (ontwikkel- of aanschaf)kosten als periodieke beheerkosten met zich meebrengt. Een dergelijke voorziening zou idealiter worden ondergebracht bij een geschikte beheerorganisatie. Hoewel dit losstaat van het toepassen van een SBOM-standaard, kan het bijdragen aan de brede adoptie en praktische toepasbaarheid ervan binnen de overheid.

De standaarden overlappen niet met andere standaarden op de ‘Pas toe of leg uit’ lijst of lijst aanbevolen standaarden. CycloneDX en SPDX hebben onderling wel een overlappende functionaliteit, maar geen conflict met de bestaande standaarden op de ‘Pas toe of leg uit’ lijst of lijst aanbevolen standaarden.

Beide standaarden brengen voor zover bekend geen veiligheidsrisico’s met zich mee. Een potentieel risico kan ontstaan als een SBOM openbaar beschikbaar worden gesteld, doordat kwetsbare componenten zichtbaar worden voor kwaadwillenden.

5.2 Open standaardisatieproces

In deze paragraaf worden het open standaardisatieproces voor beide standaarden SPDX en CycloneDX afzonderlijk beschreven.

5.2.1 SPDX

Het standaardisatieproces van SPDX staat open voor iedereen om aan deel te nemen. De specificaties van SPDX zijn vrij beschikbaar, met toegang via de Specifications - SPDX. De standaard wordt beheerd door een onafhankelijke non-profitorganisatie, The Linux Foundation. The Linux Foundation kent een open manier van vrijgave van nieuwe versies. Voor het vrijgeven van een nieuwe versie vindt een publieke consultatie plaats.

Het standaardisatieproces van The Linux Foundation is openbaar beschikbaar. De besluitvorming is open voor iedereen die wil participeren en er vindt geen besluitvorming plaats vanuit specifieke belangen, anders dan de belangen die de deelnemers zelf inbrengen. Er worden geen specifieke belangen van de Nederlandse overheid vertegenwoordigd bij de ontwikkeling van de standaarden, anders dan die ingebracht worden door de participanten.

SPDX is gepubliceerd onder de Creative Commons Attribution 3.0 Unported-licentie. Dit betekent dat de standaard royalty-free beschikbaar is voor iedereen. De financiering van het beheer van SPDX is niet gegarandeerd voor ten minste drie jaar, maar wordt wel actief ondersteund door verschillende multinationals. SPDX hangt onder de vlag van The Linux Foundation die op dezelfde manier door diverse leveranciers wordt ondersteund.

Er is op dit moment geen duidelijke nationale regie partij die de waarden en belangen van Nederlandse overheid behartigd bij The Linux Foundation voor SPDX.

5.2.2 CycloneDX

Het standaardisatieproces van CycloneDX staat open voor iedereen om in te participeren. De specificaties van CycloneDX zijn vrij beschikbaar via de CycloneDX Specification Overview. De standaard wordt beheerd door een onafhankelijke non-proforganisatie, OWASP. OWASP wordt door de community bestuurd. Vrijgave van nieuwe versies kent een open proces. Voor het vrijgeven van een nieuwe versie vindt een publieke consultatie plaats.

Het standaardisatieproces van OWASP is openbaar beschikbaar. De besluitvorming is open voor iedereen die wil participeren en er vindt geen besluitvorming plaats vanuit specifieke belangen, anders dan de belangen die de deelnemers zelf inbrengen. Er worden geen specifieke belangen van de Nederlandse overheid vertegenwoordigd bij de ontwikkeling van de standaarden, anders dan die ingebracht worden door de participanten.

CycloneDX wordt gepubliceerd onder de Apache 2.0-licentie. Dit betekent dat de standaard royalty-free beschikbaar is voor iedereen.

Informatie en gebruik van de standaard is beschikbaar via OWASP. OWASP heeft een Nederlands Chapter waar kennis over CycloneDX wordt gedeeld.

De financiering van het beheer van CycloneDX is niet gegarandeerd voor ten minste drie jaar, maar wordt wel actief ondersteund door diverse multinationals. Zie o.a. de CycloneDX Supporters. Meerdere leveranciers bieden ondersteuning voor CycloneDX.

Er is op dit moment geen duidelijke nationale regie partij die de waarden en belangen van Nederlandse overheid behartigd bij OWASP voor CycloneDX.

5.3 Draagvlak

Diverse overheidsorganisaties maken gebruik van CycloneDX en/of SPDX, zoals de Belastingdienst: CycloneDX (v1.5), Algemene Zaken: CycloneDX (v1.6). Daarnaast is het UWV bezig met het implementeren van een SBOM-standaard.

Het Nationaal Cyber Security Centrum (NCSC) raadt samen met Nederlandse organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO) het gebruik van SBOMS aan om de transparantie van de software supply chain te vergroten en de beveiliging te versterken.

Naast de indienende partijen ondersteunt ook Ministerie van Algemene Zaken een verplichting van de standaard.

Het is goed om op te merken dat het aanleveren van een SBOM is in de Verenigde Staten per presidentieel decreet verplicht gesteld voor leveranciers van softwareproducten en -diensten aan de Amerikaanse federale overheid. Verder is het gebruik van SBOMs verplicht gesteld in de Europese Cyber Resilience Act. Deze stelt echter geen verplichting aan welk SBOM-standaard te gebruiken.

5.4 Opname op de lijst bevordert adoptie

Opname van CycloneDX en SPDX op de lijst bevordert de adoptie van deze standaarden doordat het bekendheid vergroot, de vrijblijvendheid wegneemt en eenduidigheid stimuleert in het beschrijven van softwarecomponenten in ingekochte en zelfontwikkelde softwareproducten. Dit vergemakkelijkt hergebruik binnen de overheid en versterkt de onderhandelingspositie richting leveranciers.

Toch is opname op dit moment risicovol. Europese harmonisatie is nog gaande. Het nu verplicht stellen of aanbevelen van een specifieke standaard kan leiden tot dubbele implementatiekosten en verminderde interoperabiliteit als de EU later een andere standaard voorschrijft.

Bovendien zijn er inhoudelijke belemmeringen: er is niet één eenduidige, breed geaccepteerde standaard of profiel, wat leidt tot versnippering en mogelijk onduidelijkheid in gebruik. Daardoor dragen de aangemelde SBOM-standaarden in hun huidige vorm nog onvoldoende bij aan de oplossing van het probleem: het gebrek aan inzicht in softwarecomponenten.

6 Praktijkvoorbeeld

Belastingdienst

De Belastingdienst maakt gebruik van CycloneDX om het beheer van kwetsbaarheden in intern ontwikkelde (web)applicaties inzichtelijker te maken en gerichter aan te pakken. Ontwikkelteams van de Belanstingdienst genereren een SBOM van hun applicatie bij elke release. Deze worden vervolgens geüpload naar OWASP Dependency Track (een opensource applicatie voor SBOMS).

Dit proces geeft de organisatie breder inzicht in welke security kwetsbaarheden van toepassing zijn op intern draaiende softwareproducten binnen de dienst. Hiernaast geeft het ook inzicht in welke licenties op deze softwarecomponenten van toepassing zijn, en kan de Belastingdienst op dit vlak dus ook beter sturen. In de toekomst wordt verwacht dat dit proces ook ingezet kan worden om bijvoorbeeld cryptografie gebruik in onze intern ontwikkelde applicaties inzichtelijk te maken, om zo ook te zorgen dat we kunnen sturen op de quantum computer dreiging op het gebied van cryptografie. Alle bovenstaande gebruiken helpen mee aan de cyber security bescherming van de organisatie.

Algemene Zaken (DPC)

De Dienst Publiek en Communicatie (DPC) is verantwoordelijk voor het beheer, de inhoud en de toegankelijkheid van diverse websites van de Rijksoverheid, zoals Rijksoverheid.nl. Dit houdt in dat DPC zorgt voor betrouwbare en begrijpelijke informatievoorziening aan burgers, en erop toeziet dat deze websites gebruiksvriendelijk en goed toegankelijk zijn voor iedereen. SBOMS zijn bij DPC een schakel in het kwetsbaarhedenbeheer en patchmanagement.

DPC DevOps teams genereren SBOMS bij elke release van software naar Productie-omgevingen. Dit gebeurt een aantal keren per week of zelfs dagelijks. DPC maakt SBOMS van de applicatie-code maar ook van de gebruikte containers. Deze SBOMS worden naar de applicatie DependencyTrack gestuurd.

DependencyTrack matcht al deze softwarecomponenten tegen diverse openbare kwetsbaarhedenfeeds met Common Vulnerabilities and Exposures (CVE's). Een CVE is een unieke identificatiecode voor een bekende kwetsbaarheid in software of hardware. Ook is er een koppeling met de kwetsbaarhedenfeed van het NCSC, waarin openbare en niet-openbare bronnen zijn opgenomen. Zodra een kwetsbaarheid in een software-component gevonden is, krijgen de verantwoordelijke DevOps teams direct een melding in hun teamsoftware. De teams starten dan meteen een analyse en voeren mitigaties uit als dat noodzakelijk is, afhankelijk van de ingeschatte risico's van de kwetsbaarheid.

Hiermee bereikt DPC:

- Een volledig up-to-date, doorzoekbaar overzicht van alle software-componenten en dependencies zoals in gebruik op de productiesystemen, zowel applicatiecode als alle container software, per project.

- Een volledig up-to-date overzicht van gebruikte software licenties op de productiesystemen, per project.
- Een controle die elk uur wordt uitgevoerd op zowel openbare als nog niet-openbare kwetsbaarheden van alle gebruikte softwareproducten, zodat mitigerende maatregelen snel kunnen worden genomen zodra dat nodig is. Dit vormt een aanvulling op het reguliere patchmanagement van alle software.