Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Hoe breng ik mijn rechtstreekse leveranciers in kaart?

Aan de slag met het voorbereiden op de NIS2-richtlijn

Ook jouw organisatie is afhankelijk van leveranciers. Als één van de leveranciers getroffen wordt door een cyberaanval kan dat grote gevolgen hebben voor jouw organisatie. Het is daarom van belang om bewust om te gaan met de risico's uit de leverancierskeketen. Een eerste stap is het in kaart brengen van jouw leveranciers.
Deze handreiking helpt jouw om een overzicht te maken van jouw leveranciers en vervolgens te analyseren welke leveranciers het belangrijkst zijn voor jouw organisatie. Dit is een eerste stap in beheersen van risico's uit de leverancierskeketen. [1] Ben je al wat verder gevorderd dan raden we aan het document "Omgaan met risico's in de toeleveringsketen" te lezen waar good practices van Nederlandse organisaties zijn verzameld.[2]

Achtergrond

De afgelopen jaren zien we dat diverse ontwikkelingen in toenemende mate de veiligheid van onze maatschappij en economie onder druk zetten. Denk daarbij aan COVID-19, de oorlog in Oekraïne en cyberdreigingen. In het licht van deze ontwikkelingen is er sinds 2020 vanuit de Europese Unie gewerkt aan de Network and Information Security (NIS2) directive. Deze richtlijn is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. In Nederland zal de NIS2-richtlijn geïmplementeerd worden in de vorm van de Cyberbeveiligingswet.

De Rijksoverheid adviseert organisaties om niet af te wachten totdat de wet- en regelgeving volledig duidelijk is. De risico's die organisaties en systemen lopen, zijn er immers nu ook al. Organisaties die nu al in actie komen beveiligen zich niet alleen tegen deze bestaande risico's, maar zijn straks ook beter voorbereid op de komst van de nieuwe wetgeving.

Deze publicatie maakt onderdeel uit van een publicatiereeks en biedt praktische handvatten voor het uitvoeren van een risicoanalyse in het kader van de NIS2-richtlijn.[3]

Het doel van deze publicatie is om jouw organisatie te ondersteunen bij de voorbereiding op de NIS2-richtlijn. Deze publicatie biedt geen officiële of juridische basis voor jouw organisatie om aan de NIS2-richtlijn te voldoen.

NIS2

De (toeleverings)keten komt duidelijk naar voren in de NIS 2.

NIS2-wetgeving schrijft voor dat organisaties die onder deze wet vallen "*passende en evenredige technische, operationele en organisatorische maatregelen nemen*" o.a. voor "*de beveiliging van de toeleveringsketen, met inbegrip van beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners*"

Doelgroep

Deze publicatie richt zich op organisaties die onder de NIS2-richtlijn vallen en is geschreven voor personen die binnen deze organisaties een rol hebben bij security aspecten van leveranciersmanagement in het kader van de zorgplicht onder de NIS2-richtlijn.

Aan deze publicatie hebben bijgedragen

Nederlandse Spoorwegen (NS), Digital Trust Center (DTC), Siemens, Ministerie van Infrastructuur en Waterstaat (I&W), Rijksinspectie Digitale Infrastructuur (RDI) en Stichting Z-Cert.

[1] Supply Chain | Wat kun je zelf doen? | Nationaal Cyber Security Centrum (ncsc.nl)

[2] Omgaan met risico's in de toeleveringsketen | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)

[3] Bereid je voor op de wet | Over het NCSC | Nationaal Cyber Security Centrum

Wie zijn jouw rechtstreekse leveranciers?

Rechtstreekse leveranciers zijn de leveranciers waar de organisatie een contractuele relatie mee heeft. Vaak is het aantal leveranciers groot, hierdoor kan het overzicht al snel kwijt zijn. Het is van belang om een leveranciersoverzicht te maken en vervolgens te bepalen wat de belangrijkste leveranciers zijn voor de organisatie. Belangrijk is om hierbij zo veel mogelijk aansluiten bij bestaande processen (als deze bestaan). Voorbeelden van zulke processen zijn risicomanagement en leveranciersmanagement.

In deze publicatie richten we ons specifiek op de rechtstreekse toeleveranciers. In het geval dat het duidelijk is dat er grote risico's zijn bij de toeleveranciers van jouw rechtstreekse leveranciers, is van het belang om deze leverancier ook mee te nemen in het leveranciersoverzicht.

Stap 1: Maak een leveranciersoverzicht

Om zicht te krijgen op jouw rechtstreekse toeleveranciers, heb je een overzicht nodig. Er zijn tenminste drie opties om tot zo'n leveranciersoverzicht te komen:

Optie 1: een bestaand leveranciersoverzicht gebruiken

Ook andere afdelingen hebben een belang bij een leveranciersoverzicht. Daarom is de kans groot dat er al zo'n overzicht is binnen jouw organisatie. In de meeste gevallen gaat het hier om de inkoopafdeling. Andere benamingen van deze afdeling zijn purchasing of procurement. Deze afdeling is doorgaans verantwoordelijk voor het proces en de coördinatie van de inkoop van externe producten en diensten. Daardoor is de kans groot dat hier een leveranciersoverzicht aanwezig is.

Optie 2: op basis van financiële gegevens een leveranciersoverzicht maken

Mocht er geen leveranciersoverzicht en deze ook niet binnenkort beschikbaar zijn, is er ook een meer indirecte manier om een overzicht te krijgen. De meeste leveranciers sturen een factuur nadat een dienst of product geleverd is. Vervolgens worden deze facturen door jouw organisatie betaald. Dit gebeurt vaak door het financiële of crediteuren afdeling. Een deel van de uitgaande gelden zijn betalingen van facturen van toeleveranciers. Door de betalingen van het afgelopen jaar te analyseren, kan jij in kaar brengen wie jouw toeleveranciers zijn.

Optie 3: op basis van assets een leveranciersoverzicht maken

Een andere manier om jouw toeleveranciers in kaart te brengen is aan de hand van een overzicht van de producten en diensten die jouw organisatie gebruikt. Dit wordt ook wel "*assets*" genoemd. Een overzicht van je assets kan je bijvoorbeeld vinden in een asset managementsysteem of een Configuration Management Database (CMDB). Op basis van deze overzichten kun je vervolgens in kaart brengen welke leveranciers bepaalde assets leveren en zo tot een leveranciersoverzicht komen.

Mocht er geen overzicht van de assets zijn, dan is het een belangrijke stap om deze alsnog in kaart te brengen. Doe dit samen met andere teams binnen de organisatie die hier inzicht in hebben. Je kan dit bijvoorbeeld doen aan de hand van workshops of door het gebruik van bepaalde tools.[4]

Stap 2: Maak afspraken over het actueel houden van het leveranciersoverzicht

Maak duidelijke afspraken over de verantwoordelijkheden voor het leveranciersoverzicht. Hoe de verschillende verantwoordelijken uiteindelijk worden verdeeld hangt sterk af van de cultuur en structuur van de organisatie. Je kan dit doen aan de hand van een RASCI-matrix.[5]

Belangrijk is dat er uiteindelijk één persoon "*accountable*" en één persoon "*responsible*" is. Dit zal vaak betekenen dat de security verantwoordelijk niet diegene is die het leveranciersoverzicht onderhoudt, wel heeft deze een belang bij een goed overzicht. In veel gevallen zal een directeur (van de inkoop of financiële afdeling) "*accountable*" zijn voor het leveranciersoverzicht; is een medewerker (van de inkoop of financiële afdeling) "*responsible*"; en zal risicomanager of security verantwoordelijke "*consulted*" worden voor het security aspect van leveranciersoverzicht. Zoals eerder benoemd, zullen de verantwoordelijkheden niet bij elke organisatie hetzelfde zijn verdeeld. Dit hangt sterk af van de cultuur en structuur van de organisatie en is dus overal anders.

Nadat de verantwoordelijkheden zijn vastgesteld, kunnen er afspraken worden gemaakt over het proces van onderhoud van het leveranciersoverzicht. Bijvoorbeeld dat

[4] Zie ook de website van NCSC-UK voor meer informatie over assets en asset management: https://www.ncsc.gov.uk/collection/10-steps/asset-management en https://www.ncsc.gov.uk/guidance/asset-management

[5] RACI-model - Wikipedia

er jaarlijks een update van het leveranciersoverzicht wordt uitgevoerd door diegene die "*responsible*" is.

Een volgende stap is om alle afspraken te formaliseren door deze te laten goedkeuren door een directeur of directieteam. Zorg ervoor dat dit schriftelijk wordt vastgelegd.

Let op!

In stap 2 hebben we het over de verantwoordelijkheden omtrent het leveranciers**overzicht** en niet over de verantwoordelijkheden omtrent het bredere leveranciers**management**.

Leveranciers**management** gaat niet alleen over het maken en onderhouden van een overzicht, maar bijvoorbeeld ook over het selecteren van een leverancier en het onderhouden van de relatie. Doorgaans is de business hier "*accountable*" aangezien zij de gebruiker zijn en over de inhoudelijke kennis beschikken om tot een goede behoeftestelling te komen. De inkoopafdeling heeft hier vaak een rol als procesbegeleider en coördinator. Al verschilt dit uiteraard weer per organisatie.

Stap 3: Classificeer en prioriteer jouw leveranciers

Een lange lijst met alle leveranciers biedt overzicht, maar nog geen inzicht in welke leveranciers het belangrijkst zijn voor jouw organisatie. Daarom is de volgende stap om te de leveranciers te classificeren en prioriteren op basis van het belang voor jouw organisatie. Dit kun je doen op basis van de volgende factoren:

1) De mate van afhankelijkheid van een leverancier voor de beschikbaarheid, integriteit en vertrouwelijkheid van de Te Beschermen Belangen (TBB, ook bekend als kroonjuwelen) van de organisatie: als onderdeel van het risicomanagementproces heeft de organisatie in kaart gebracht wat de TBB's zijn. Is dat nog niet gedaan of is het onduidelijk wat de TBB's zijn? Lees dan eerst de publicatie hierover.[6]
   Bepaal vervolgens voor de 10 belangrijkste TBB's welke leveranciers hier belangrijk voor zijn. Het is belangrijk om in ieder geval twee soorten leveranciers te onderscheiden:
   a) Leveranciers die essentieel zijn voor de business continuiteit, het primaire proces zelf.[7] Bijvoorbeeld een autofabrikant die een toeleverancier heeft die de banden van de auto levert. Als deze leverancier geen banden meer levert, kan de auto ook niet worden afgemaakt
   b) Een leverancier die een IT-asset leveren en onderhouden dat een belangrijk onderdeel is van één van de TBB's.

2) Denk ook na over leveranciers die toegang hebben tot vertrouwelijke systemen en/of data: Bepaalde leveranciers leveren een niet kritieke dienst of product aan uw organisatie, maar hebben wel toegang tot vertrouwelijke systemen en/of data. Neem hier ook leveranciers mee waar jouw organisatie zelf vertrouwelijke data naar stuurt omdat zij een dienst voor jou verrichten.

3) Leveranciers met een slechte reputatie: over welke leveranciers maak je je zorgen vanwege een slechte reputatie? Deze leveranciers verdienen mogelijk extra aandacht omdat er binnen de organisatie, of bij jouw partners, slechte ervaringen mee bestaan. Ook als een leverancier betrokken is bij een informatiebeveiligingsincident zoals een datalek kan dat een aanleiding zijn om deze leverancier te prioriteren.

Documenteer deze risicogerichte analyse. Indien bij deze selectie ook al een aantal toeleveranciers van jouw rechtstreeks leveranciers in het vizier heeft, neem deze dan meteen mee in de analyse.

[6] https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-breng-ik-mijn-dreigingen-in-kaart

[7] U kunt ook gebruik maken van een Kraljic matrix om te bepalen van welke leveranciers u het meest afhankelijk bent. Zie https://en.wikipedia.org/wiki/Kraljic_matrix

80-20 regel

Voor organisaties die nog geen of beperkt zicht hebben op hun leveranciers en de risico's die daaruit voortkomen, is het zaak om in deze eerste inventarisatie niet te hoge eisen te stellen aan het leveranciersoverzicht. Een eerste lijst met leveranciers die op basis van bovenstaande drie aspecten zijn geïnventariseerd, is in deze eerste stap een prima resultaat en een goede basis voor verdere aanvullingen. Waarschijnlijk is hiermee al 80% van het hoog risico leveranciers inzichtelijk gemaakt. Vergeet vervolgens niet om ook de laatste 20% in kaart te brengen. Ook hier kan nog een significant risico uit voorkomen.

Stap 4: Onderhouden van de classificering en prioritering van leveranciers

Ook de classificering en prioritering van het leveranciersoverzicht (zoals beschreven in stap 3) kan veranderen. De volgende twee redenen kunnen daar een aanleiding voor zijn:

1. Een verandering in het leveranciersoverzicht, bijvoorbeeld door een faillissement, waardoor een leverancier weg valt. Een andere voorbeeld is het contracteren van een nieuwe leverancier, waardoor er een leverancier bijkomt.
2. Een verandering in de context rondom de organisatie, waardoor er nieuwe of veranderende risico's zijn. Een voorbeeld zijn de geopolitiek spanningen waardoor banden met leveranciers uit bepaalde landen worden heroverwogen.

Probeer bij eventuele veranderingen in het leveranciersoverzicht zoveel mogelijk aan te sluiten bij het ritme en de frequentie van gerelateerde processen, zoals het risicomanagement proces. Dit gebeurt doorgaans ten minste 1 keer per jaar. Mocht het nodig zijn dit vaker te doen is dit uiteraard ook mogelijk.

Als laatste helpt het om een warme band met de inkoopafdeling te onderhouden. Zij kunnen de rest van de organisatie tijdig informeren over eventuele veranderingen van leveranciers. Hierdoor heeft de organisatie voldoende tijd om zich hierop voor te bereiden.

Meer weten?

Wil je meer weten of ben je al toe aan een volgende stap om meer in detail de leveranciersrisico's te analyseren? Kijk dan ook eens naar de kennisproducten van onze kennispartners:

- NCSC-UK: How to assess and gain confidence in your supply chain... - NCSC.GOV.UK
- NCSC-UK: Mapping your supply chain - NCSC.GOV.UK
- ENISA – Good Practices for Supply Chain Cybersecurity — ENISA (europa.eu)
- Cyra: Cyra - jouw route naar digitale weerbaar ondernemen (cyberrating.nl)
- Z-CERT: Kennisbank – Z-CERT
- DTC: Bescherm je organisatie tegen supply chain aanvallen | Digital Trust Center (Min. van EZK)
- DTC: Risicoklasse-indeling Digitale Veiligheid Risicoklasse-indeling Digitale Veiligheid (digitaltrustcenter.nl)

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

juli 2024