Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Hoe breng ik mijn dreigingen in kaart?

Aan de slag met het voorbereiden op de NIS2-richtlijn

Factsheet FS 2024 | versie 0.9 | juli 2024

Deze publicatie biedt praktische handvatten voor jouw organisatie om dreigingen in kaart te brengen ter voorbereiding op de NIS2-richtlijn. De NIS2-richtlijn bevat een zorgplicht die jouw organisatie verplicht om een risicoanalyse uit te voeren. Op basis van deze risicoanalyse kun je beoordelen wat passende maatregelen zijn om de continuïteit van diensten te waarborgen en informatie te beschermen.

Het in kaart brengen van relevante dreigingen is onderdeel van een risicoanalyse. Deze publicatie helpt je bij het zetten van de eerste stappen voor het onderdeel dreiging. Lees voor de andere onderdelen ook de publicaties 'Hoe breng ik mijn te beschermen belangen in kaart' en 'Hoe krijg ik grip op mijn security controls'? om een tot afgeronde risicobeoordeling te kunnen komen.

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.[1]

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.[2] De handvatten in deze publicatie zijn ter voorbereiding op de NIS2-richtlijn geschreven, maar kunnen ook breder worden toegepast om dreigingen in kaart te brengen.[3]

Doelgroep

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

Wat is een dreiging?

Onder dreiging verstaan we iets wat gevaar of schade kan opleveren voor een organisatie. Dit kan bijvoorbeeld leiden tot verstoring, reputatieschade of financieel verlies.[4] Er bestaan verschillende actoren met uiteenlopende intenties die een cyberdreiging voor jouw organisatie kunnen vormen. Denk hierbij bijvoorbeeld aan criminelen, hacktivisten, insiders of statelijke actoren.

De implementatie van de NIS2-richtlijn levert een belangrijke bijdrage aan het doel dat organisaties zicht hebben op cyberdreigingen en risico's en dat zij daar op een passende manier mee omgaan.

Deze publicatie biedt een stappenplan om op een gestructureerde manier zicht op cyberdreigingen te krijgen. Het doel van dit stappenplan is om jouw organisatie te helpen bij het zetten van de eerste stappen.

[1] Cyberbeveiligingswet (NIS2-richtlijn) | Over het NCSC | Nationaal Cyber Security Centrum

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

[3] Het doel van deze publicatie is om organisaties te ondersteunen bij de voorbereiding op de NIS2-richtlijn. Deze publicatie biedt geen officiële of juridische basis om aan de NIS2-richtlijn te voldoen

[4] Woordenboek - Cyberveilig Nederland

Stap 1: Bereid het gesprek met je bestuur voor

Om cyberdreigingen in kaart te kunnen brengen, moet er doorgaans extra tijd en capaciteit vrijgemaakt worden. Hiervoor heb je de steun van het bestuur nodig[5]. We adviseren als eerste stap om dit gesprek voor te bereiden. Dit kun je bijvoorbeeld doen door:

1. In gesprek te gaan met personen binnen jouw organisatie die over dreigingsinformatie beschikken. Dit zijn bijvoorbeeld de personen die zich met risicomanagement processen bezig houden, maar ook de technisch experts of de inkoopafdeling. Inventariseer met behulp van deze gesprekken in hoeverre jouw organisatie zicht heeft op cyberdreigingen. Welke informatie is al beschikbaar?
2. Het verzamelen van praktijkvoorbeelden van cyberincidenten. Dit kunnen incidenten binnen je eigen organisatie zijn, maar ook voorbeelden van incidenten bij vergelijkbare organisaties in binnen-en buitenland.
3. Het bijeenbrengen van het huidige zicht op cyberdreigingen en eventuele cyberincidenten om als input voor het gesprek met je bestuur te gebruiken.
4. Het vertalen van deze input op een heldere manier die het bestuur aanspreekt en begrijpelijk is. Dit kun je bijvoorbeeld doen door cyberdreigingen en (eerdere) cyberincidenten zo concreet en tastbaar mogelijk te maken. Hiermee laat je zien dat een dreiging niet alleen theoretisch, maar ook heel voorstelbaar of zelfs concreet kan zijn.

Stap 2: Ga in gesprek met het bestuur

In de eerste stap heb je een beeld gevormd van de mate waarin jouw organisatie nu zicht op dreigingen heeft. In deze stap ga je op basis van deze inventarisatie het gesprek met het bestuur aan en kun een plan presenteren met de middelen die je concreet nodig hebt. Het is tijdens dit gesprek ook van belang om afspraken te maken over de opvolging van de uitkomsten van dit plan. Uitgangspunten voor dit gesprek zijn bijvoorbeeld:

1. Een toelichting waarom zicht op dreigingen belangrijk als onderdeel van een risicoanalyse. Op basis van deze risicoanalyse kun je beoordelen wat passende maatregelen zijn om de continuïteit van diensten te waarborgen en informatie te beschermen. Het uitvoeren van een risicoanalyse is bovendien onderdeel van de NIS2 richtlijn.
2. Een plan presenteren om het zicht op dreigingen a) in kaart te brengen of b) te verbeteren.
3. De benodigde capaciteit en middelen toelichten. Gebruik hiervoor de input uit de eerste stap. Vraag het bestuur om het plan formeel goed te keuren.
4. Het maken van concrete afspraken om de resulaten van het plan terug te koppelen aan het bestuur. Dit is nodig om vervolgstappen te kunnen bepalen om tot een afgeronde risicoanalyse te komen.

Met de steun en formele goedkeuring van het bestuur kun je aan de slag met het zetten van de eerste stappen om cyberdreigingen in kaart te brengen of het zicht op cyberdreigingen te verbeteren.

Stap 3: Verzamel dreigingsinformatie

Om een beeld te kunnen vormen van mogelijke cyberdreigingen voor jouw organisatie, zul je dreigingsinformatie moeten verzamelen. Dit kan op verschillende manieren:

1. Inventariseer welke dreigingsinformatie er al binnen je eigen organisatie aanwezig is. Zie hiervoor ook het advies in stap één.
2. Verzamel publiek beschikbare dreigingsinformatie. Denk hierbij aan publicaties zoals het Cybersecurity Beeld Nederland (CSBN), het AIVD jaarverslag of het Dreigingsbeeld Statelijke Actoren. Ook commerciële cybersecurity bedrijven brengen openbaar beschikbare dreigingsrapporten uit.
3. Bekijk openbare dreigingsinformatie die wordt gedeeld door het Nationaal Cyber Security Centrum (NCSC) of het Digital Trust Centre (DTC).
4. Verken of andere organisaties binnen jouw sector bereid zijn om dreigingsinformatie uit te wisselen.
5. Het inkopen van dreigingsinformatie bij commerciële bronnnen. Verschillende marktpartijen bieden deze diensten aan. Overweeg of deze informatie van toegevoegde waarde voor jou organisatie is.
6. Maak op basis van de verzamelde dreigingsinformatie een overzicht van de verschillende dreigingsactoren en de bijbehorende intenties.

[5] https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/besturen/10-vragen-aan-je-ciso

Door dreigingsinformatie te verzamelen kun je het bestaande beeld van cyberdreigingen verruimen. Om vervolgens te bepalen welke dreigingen het meest relevant voor jouw organisatie zijn, kun je een workshop organiseren. Dit wordt toegelicht in de volgende stap.

Stap 4: Organiseer een workshop

Het organiseren van een workshop is een praktische manier om af te wegen welke cyberdreigingen het meest relevant voor jouw organisatie zijn. Door verschillende expertises bij elkaar te brengen kun je vanuit meerdere invalshoeken tot een volledige en gedeeld dreigingsbeeld komen.

Nodig hiervoor de interne stakeholders uit die je ook in de vorige stappen hebt bevraagd. Je kunt overwegen om externe (dreigings-) experts uit te nodigen, maar het is in dit geval belangrijk om op voorhand afspraken over de vertrouwelijkheid van de sessie te maken. Voor de inhoudelijke invulling en opzet van de workshop kun je denken aan:

1. Het toesturen van een overzicht van mogelijke dreigingsactoren en bijbehorende intenties die je hebt verzameld in stap 3 voorafgaand aan de workshop. Vraag de deelnemers om zich alvast in te lezen zodat ze een beeld hebben van mogelijke cyberdreigingen.
2. Bespreek tijdens de workshop in aparte tijdsblokken deze dreigingsactoren en bijbehorende intenties. Houd de tijd goed in de gaten en ook het onderwerp van het betreffende tijdsblok. Dit is noodzakelijk om tot bruikbaar eindresultaat te komen.
3. Vraag in het eerste tijdsblok aan de deelnemers om, individueel en zonder te communiceren, een rangschikking te maken van de verschillende dreigingsactoren op basis van de intentie van deze actor en op basis van de eigen kennis over de organisatie. Hierbij is het doorgaans ook belangrijk om kennis te hebben van de te beschermen belangen van jouw organisatie[6]. Nadat alle deelnemers individueel een rangschikking hebben aangebracht, vraag je de deelnemers om hun eigen rangschikking voor alle deelnemers toe te lichten en te onderbouwen. Bied voldoende ruimte voor discussie. Sluit het blok af door vervolgens tot een gedeelde rangschikking te komen. Leg hierbij ook de onderbouwing van de keuzes vast.
4. Vraag tijdens het tweede tijdsblok aan de deelnemers om hetzelfde te doen voor de meest voorstelbare aanvalsmethoden. Gebruik hiervoor de vastgestelde rangschikking van dreigingsactoren. Vraag wederom eerst om een individuele inschatting en vraag de deelnemers vervolgens om de inschatting voor alle andere deelnemers toe te lichten. Bied voldoende ruimte voor discussie en vraag de deelnemers om tot een gedeelde inschatting te komen.
5. Vat de bevindingen samen en sluit de workshop af.

Met behulp van een workshop kun je focus aanbrengen om een meer gerichte inschatting te maken van de meest relevante dreigingsactoren en aanvalsmethoden voor jouw organisatie. Verwerk de bevindingen en bijbehorende onderbouwingen in een overzicht voor het bestuur van je organisatie.

Stap 5: Communiceer de resultaten aan je bestuur en bepaal vervolgstappen

Met behulp van de resultaten en het overzicht in de vorige stap kun je weer met het bestuur in gesprek gaan. Vermijd bij voorkeur technisch jargon en probeer de resultaten sprekend te maken door concrete en sprekende voorbeelden uit de workshop aan te halen of voorstelbare scenario's te schetsen. Houdt het eenvoudig en overzichtelijk.

Benadruk dat zicht op dreigingen een belangrijke stap is, maar nog geen afgeronde risicoanalyse betreft. Hiervoor moeten de cyberdreigingen afgewogen worden tegen de te beschermen belangen van de organisatie[7] en moet ook het huidige niveau van weerbaarheid[8] in kaart worden gebracht.
Bespreek tot slot met je bestuur welke vervolgstappen er nodig zijn om tot een afgeronde risicoanalyse te komen en wat je hiervoor nodig hebt.

[6] https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-breng-ik-mijn-te-beschermen-belangen-in-beeld

[7] https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/herkennen/hoe-breng-ik-mijn-te-beschermen-belangen-in-beeld

[8] https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/beschermen/grip-op-security-controls

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