Hanze

share your talent.
move the world.

Cybersecurity voor het mkb: van Europese wetgeving naar regionale inbedding

Inzichten die de praktijk in Noord-Nederland versterken

Redactie: mr. P. M. Piest, mr. dr. T. Mulder

Cybersecurity voor het mkb: van Europese wetgeving naar regionale inbedding

Inzichten die de praktijk in Noord-Nederland versterken

Redactie: mr. P. M. Piest, mr. dr. T. Mulder

Juli 2025

@ Hanze 2025

Inhoudsopgave

Inleiding

De digitale wereld ontwikkelt zich in een razendsnel tempo. Overheden, bedrijven en burgers worden dagelijks geconfronteerd met nieuwe technologieën, digitale processen en de regelgeving die daarmee gepaard gaat. Hoewel digitale regels vaak op nationaal, en meestal zelfs op Europees niveau worden opgesteld, is hun impact voelbaar tot in de haarvaten van de regio. Hoe gaat het midden- en kleinbedrijf (hierna: mkb) om met digitale verplichtingen en digitale veiligheid? Waar wringt het in de uitvoering? En welke innovatieve oplossingen worden er door studenten op lokaal niveau ontwikkeld om recht te doen aan zowel de letter van de wet als de praktijk van het mkb?

Door inzichten uit de regio te bundelen, willen we laten zien dat digitale transitie niet alleen een technische of juridische uitdaging is, maar vooral ook een kwestie van samenwerking, aanpassingsvermogen en regionaal maatwerk. De ervaringen die u in dit boek leest, bieden geen pasklare antwoorden, maar wel inspiratie en richting. Er is een selectie gemaakt uit een aantal recente afstudeeronderzoeken en bijbehorende beroepsproducten van studenten (of inmiddels alumni) van de Hanze in Groningen. Deze afstudeeronderzoeken richting zich op de volgende onderwerpen: de NIS2-richtlijn en de Cyber Resilience Act.

De NIS2-richtlijn (oftewel: *Network and Information Security Directive*) is de vernieuwde Europese richtlijn voor cyberbeveiliging. Deze opvolger van de oorspronkelijke NIS1-richtlijn heeft als doel de digitale weerbaarheid van vitale sectoren binnen de Europese Unie te vergroten. NIS2 stelt strengere eisen aan organisaties op het gebied van risicobeheer, incidentmelding en beveiligingsmaatregelen. Nieuw is dat de richtlijn voor meer sectoren en organisaties geldt, waaronder ook het mkb in sommige gevallen.

De Cyber Resilience Act is een Europese verordening die tot doel heeft de cyberbeveiliging van digitale producten en software binnen de Europese Unie structureel te verbeteren. Fabrikanten en ontwikkelaars worden verplicht om al vanaf het ontwerp van het product rekening te houden met cyberveiligheid en om eventuele kwetsbaarheden voor te zijn of anders te verhelpen zodra ze worden ontdekt. Deze wetgeving geldt voor een breed scala aan producten met digitale elementen, van slimme apparaten tot industriële software. Door uniforme regels in te voeren,

wil de Europese Unie consumenten beter beschermen en bedrijven duidelijkheid geven over hun verantwoordelijkheden. De verordening treedt vanaf 2025 gefaseerd in werking.

Een belangrijke schakel in dit boek is Cyber Security Noord-Nederland (hierna: CSNN). CSNN is een regionaal samenwerkingsverband dat zich richt op het versterken van digitale weerbaarheid in Noord-Nederland. Door kennisdeling, onderzoek en praktijkgerichte projecten brengt CSNN overheden, bedrijven, onderwijsinstellingen en maatschappelijke organisaties samen rond actuele vraagstukken op het gebied van cyberveiligheid en digitale regelgeving. Vanuit deze regionale verbondenheid en expertise draagt CSNN bij aan het vergroten van bewustwording én het ontwikkelen van praktische oplossingen die passen bij de unieke kenmerken van regio Noord-Nederland. In dit boek nemen we u aan de hand van onderzoek, uitgevoerd door HBO-rechtenstudenten van de Hanze binnen het project Cybersecurity Noord-Nederland, mee in de wisselwerking tussen digitale regelgeving en regionale praktijk.

Het Programma CSNN is mede mogelijk gemaakt door bijdragen van provincie Groningen (RSP-middelen) en gemeente Groningen. Dankzij deze steun is het mogelijk geworden om regionale kennis en ervaringen te bundelen en breder beschikbaar te maken voor iedereen die zich bezighoudt met digitale regelgeving in samenhang van de praktijk. Wij danken hen daar hartelijk voor.

Bij de totstandkoming van dit boek leverden het lectoraat Juridische Aspecten van het Ondernemerschap en de Digital Society Hub van de Hanzehogeschool Groningen een waardevolle bijdrage. Het lectoraat doet praktijkgericht onderzoek naar de juridische uitdagingen waar ondernemers mee te maken krijgen in een snel digitaliserende samenleving, en draagt bij aan kennisontwikkeling op het snijvlak van recht, technologie en ondernemerschap. De Digital Society Hub fungeert als innovatielab waar studenten, onderzoekers, bedrijven en maatschappelijke organisaties samenwerken aan digitale vraagstukken. In deze dynamische omgeving worden theorie en praktijk verbonden, met oog voor de impact van digitale regels op de regio.

Welkom in een wereld waar digitale regels en regionale realiteit elkaar ontmoeten. We hopen dat de inzichten en ervaringen in dit boek inspireren, aan het denken zetten en bijdragen aan een beter begrip van de digitale uitdagingen én kansen in de regio. Of u nu werkzaam bent in beleid, praktijk, onderzoek of onderwijs — voor iedereen die te maken heeft met digitale regels in een veranderende wereld valt hier iets te halen.

Wij wensen u veel leesplezier.

mr. P. M. Piest
mr. dr. T. Mulder

De NIS2–richtlijn

In het licht van alle digitale ontwikkelingen is er sinds 2020 vanuit de Europese Unie gewerkt aan de aanpassing van de *Network and Information Security Directive*. Deze richtlijn is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. Een richtlijn is een vorm van Europese wetgeving die bindend is voor lidstaten wat betreft het te bereiken doel, maar die lidstaten vrijheid laat in de manier waarop zij dat doel in hun eigen nationale wetgeving verwerken. Dat betekent dat een richtlijn in principe niet direct geldt voor burgers of bedrijven, maar eerst moet worden omgezet (oftewel: geïmplementeerd) in nationale wetten of regels. In Nederland wordt de NIS2-richtlijn geïmplementeerd in de vorm van de Cyberbeveiligingswet (Cbw).[1] Van de Cbw is enkel nog het concept klaar, Nederland heeft daarmee nog niet aan zijn implementatieverplichting – binnen de daartoe gestelde termijn – voldaan. We nemen daarom de verplichtingen vanuit de NIS2 vooralsnog als uitgangspunt.

Organisaties vallen automatisch onder de NIS2-richtlijn, en daarmee de toekomstige Cyberbeveiligingswet, als zij actief zijn in aangewezen sectoren en volgens bepaalde criteria gekenmerkt worden als ‘essentiële’ of ‘belangrijke’ entiteit. Automatisch wil zeggen dat de verplichtingen van de Cyberbeveiligingswet voor deze organisaties direct gaan gelden zodra de wet in werking treedt.[2] Organisaties die onder de NIS2-richtlijn vallen zijn over het algemeen middelgrote tot grote organisaties, die werkzaamheden uitvoeren met betrekking tot energie, vervoer, bankwezen, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, overheid, ruimtevaart en digitale aanbieders. Enkele concrete voorbeelden van organisaties die onder deze wetgeving vallen zijn bijvoorbeeld een ziekenhuis, een waterzuiveringsbedrijf, een telecommunicatieprovider, maar ook (onderdelen van) de centrale overheid. Een volledige lijst van organisaties die onder de NIS2-richtlijn vallen staan opgenomen in bijlage I en bijlage II van de NIS2-richtlijn.

1 ‘Cyberbeveiligingswet (NIS2-richtlijn)’, ncsc.nl
2 ‘Over de Cbw’, ncsc.nl.

De richtlijn verplicht elke lidstaat om een nationale strategie voor cyberbeveiliging op te stellen, waarin aandacht wordt besteed aan de beveiliging van de toeleveringsketen, het beheer van kwetsbaarheden en het vergroten van kennis en bewustwording over cyberbeveiliging. Daarnaast moeten lidstaten een lijst opstellen van aanbieders van essentiële diensten en deze regelmatig actualiseren om te waarborgen dat deze organisaties voldoen aan de eisen van de richtlijn. De verplichtingen die voortvloeien uit de NIS2-richtlijn kunnen onderscheiden worden in drie categorieën: de zorgplicht, de meldplicht en toezicht.

Zorgplicht
De zorgplicht uit de NIS2-richtlijn verplicht meer organisaties (ten opzichte van de NIS1-richtlijn) tot het nemen van adequate maatregelen ter bescherming van netwerk- en informatiesystemen tegen digitale dreigingen.[3] Dit betekent dat organisaties verantwoordelijk worden gehouden voor het op orde brengen en houden van hun digitale beveiliging. De centrale gedachte achter deze zorgplicht is dat organisaties proactief risico's in kaart brengen en maatregelen treffen om schade door cyberincidenten te voorkomen of te beperken. Artikel 21 van de richtlijn speelt hierin een sleutelrol. Daarin wordt beschreven dat organisaties technische, operationele en organisatorische maatregelen moeten treffen die afgestemd zijn op de aard van de risico's waarmee zij te maken kunnen krijgen. Deze maatregelen moeten niet willekeurig worden gekozen, maar gebaseerd zijn op een zorgvuldige risicoanalyse en afgestemd zijn op de specifieke dreigingen binnen hun sector en context. Voorbeelden van dergelijke maatregelen zijn het opstellen van een incident response plan, het beveiligen van de toeleveringsketen, het inrichten van back-upsystemen en herstelprocedures bij incidenten, en het trainen van personeel op het gebied van cybersecurity.[4]

Wat opmerkelijk is binnen de NIS2-richtlijn, is dat zij de verantwoordelijkheid om de zorgverplichting na te leven, niet uitsluitend bij een IT-afdeling van een organisatie legt. In artikel 23 wordt namelijk bepaald dat het bestuur of de directie (het zogeheten "leidinggevend orgaan") eindverantwoordelijk is voor het naleven van de zorgplicht. Dit betekent dat de top van de organisatie geacht wordt voldoende inzicht te hebben in de cyberrisico's die hun organisatie loopt en in de maatregelen die getroffen moeten worden. Bestuurders kunnen dus niet langer zeggen dat cybersecurity geen bestuurszaak is.

Meldplicht
De meldplicht uit de NIS2-richtlijn vormt een tweede belangrijke pijler in het Europese kader voor digitale weerbaarheid. Waar de zorgplicht vooral gericht is op preventie, richt de meldplicht zich op de fase tijdens en na een beveiligingsincident: het snel en zorgvuldig melden van incidenten die gevolgen kunnen hebben voor de dienstverlening van een organisatie. Deze meldplicht is vastgelegd in artikel 23 t/m 28 van de NIS2-richtlijn.

Wat betekent deze meldplicht in de praktijk? Als een organisatie onder de richtlijn valt en te maken krijgt met een cyberincident dat invloed kan hebben op haar dienstverlening, dan moet zij dit incident zo snel mogelijk melden. In artikel 27 wordt uitgelegd hoe deze meldplicht in de praktijk moet worden nageleefd. Denk bijvoorbeeld aan de situatie dat een ziekenhuis wordt getroffen door een ransomware-aanval. Op grond van de artikel 27 uit de richtlijn moet binnen 24 uur een melding worden gemaakt bij de bevoegde autoriteit met de dan beschikbare informatie. Binnen 72 uur volgt er vanuit het ziekenhuis een uitgebreidere melding over de impact van de aanval en de getroffen systemen. Na een maand levert het ziekenhuis vervolgens een eindrapport op, met daarin analyse en de getroffen maatregelen naar aanleiding van de eerdere aanval.

Het doel van deze meldplicht is tweeledig: enerzijds stelt het nationale autoriteiten in staat om snel te reageren, eventueel door ondersteuning of coördinatie met andere partijen; anderzijds draagt het bij aan bredere informatie-uitwisseling over cyberdreigingen en incidenten, waardoor ook andere organisaties kunnen leren van de gebeurtenis. De meldplicht is dus niet alleen een juridische verplichting, maar ook een mechanisme om het algemene cybersecurity-niveau binnen de Europese Unie te verhogen.[5]

Toezicht
De toezichtspijler van de NIS2-richtlijn vormt het sluitstuk van het Europese stelsel voor cybersecurityverplichtingen. Waar de zorgplicht de preventieve kant van beveiliging behandelt en de meldplicht ingrijpt wanneer incidenten zich voordoen, zorgt het toezichtmechanisme ervoor dat deze verplichtingen ook daadwerkelijk worden nageleefd. De toezichtstructuur binnen NIS2 is dan ook ontworpen als een combinatie van preventieve controle, actieve handhaving en stevige sanctiebevoegdheden. Deze pijler is in de richtlijn vooral uitgewerkt in de artikelen 31 t/m 38. In de NIS2 wordt een onderscheid gemaakt tussen twee categorieën van entiteiten: essentiële entiteiten en belangrijke entiteiten. Dit onderscheid is van groot belang voor het toezicht. Voor essentiële entiteiten geldt een actief en direct toezicht. Dat betekent dat de bevoegde autoriteiten proactief controles mogen uitvoeren, zoals audits, inspecties ter plaatse, en het opvragen van documentatie. Bij belangrijke entiteiten is sprake van reactief toezicht, wat inhoudt dat toezicht vooral plaatsvindt naar aanleiding van signalen, klachten of incidentmeldingen. Deze toezichtstructuur weerspiegelt het risicoprofiel van de betreffende sectoren en organisaties.

In artikel 32 van de richtlijn krijgen toezichthouders ruime bevoegdheden, waaronder: toegang eisen tot informatie over het cybersecuritybeleid en risicobeheer van een organisatie, beveiligingsmaatregelen toetsen op doeltreffendheid, audits uit te voeren, waarschuwende of bindende instructies geven en de mogelijkheid om sancties op te leggen.

Kortom, organisaties die onder de reikwijdte van de richtlijn vallen, kunnen erop rekenen dat hun aanpak kritisch wordt gevolgd, dat er bij nalatigheid wordt opgetreden, en dat toezichthouders actief betrokken zijn bij het verhogen van de algehele cyberweerbaarheid. Het is daarmee een systeem dat niet alleen handhaaft, maar ook stimuleert, begeleidt en versterkt.[6]

3 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cybersecurity in de Unie (NIS2), overweging (7, 16).
4 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cybersecurity in de Unie (NIS2), overweging (24).
5 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cybersecurity in de Unie (NIS2), overweging (101 t/m 103).
6 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cybersecurity in de Unie (NIS2), overweging (105).

Het eerste onderzoek dat in dit boek wordt gepresenteerd is een onderzoek, welke uitgevoerd is in opdracht van Cyber Security Noord-Nederland en het Lectoraat Juridische aspecten van het Ondernemerschap. Het onderzoek is gedaan door een (inmiddels) alumni van de HBO-Rechten opleiding van de Hanze. Centraal stond de vraag welke ontwerpeisen van toepassing zijn op een checklist waarmee mkb's kunnen vaststellen of zij onder de richtlijn vallen en aan welke verplichtingen zij moeten voldoen. Aan de hand van juridisch en praktijkgericht onderzoek, inclusief interviews en toetsing van een concept- checklist, is een gebruiksvriendelijke en overzichtelijke checklist ontwikkeld, die positief is ontvangen en toepasbaar blijkt binnen diverse organisaties.

Het tweede onderzoek dat in dit boek gepresenteerd wordt, is een onderzoek dat is gedaan in opdracht van het Martini Ziekenhuis Groningen. Het onderzoek is gedaan door een (inmiddels) alumni van de HBO-Rechten opleiding van de Hanze. Het onderzoek richt zich op het ontwerpen van een procedurebeschrijving voor de meldplicht van cyberincidenten binnen het Martini Ziekenhuis, in het kader van de implementatie van de NIS2-richtlijn. Deze Europese richtlijn stelt immers strengere eisen aan organisaties in vitale sectoren, waaronder de zorg, om significante cyberincidenten tijdig en gestructureerd te melden. Het doel van het onderzoek was om een meldprocedure te ontwikkelen die zowel juridisch correct als praktisch toepasbaar is voor medewerkers in alle lagen van het ziekenhuis. Door een combinatie van theoretische analyse, van onder andere de NIS2, en praktijkonderzoek via interviews en feedbacksessies met interne experts, is een bruikbaar en begrijpelijk stappenplan ontwikkeld. Het beroepsproduct biedt concrete richtlijnen, heldere verantwoordelijkheden en toegankelijke taal, en draagt zo bij aan de digitale weerbaarheid van het ziekenhuis.

mr. P. M. Piest
mr. dr. T. Mulder

Het belang van cybersecurity in de Europese Unie

Wat betekent de NIS2-richtlijn voor MKB-bedrijven?

Kayleigh Veenstra

Samenvatting

Ter afronding van de studie HBO-rechten aan de Hanzehogeschool Groningen heeft dit onderzoek plaatsgevonden. Het onderzoek is uitgevoerd in opdracht van het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen in samenwerking met Cybersecurity Noord- Nederland.

Op dit moment is de NIS1-richtlijn in werking. In Nederland is de richtlijn in de Wet Beveiliging Netwerk- en Informatie systemen geïmplementeerd. De NIS2-richtlijn wordt in Nederland ook in de Wet Beveiliging Netwerk- en Informatiesystemen geïmplementeerd. Deze wet- en regelgeving is per oktober 2024 van kracht. De NIS2-richtlijn is op meer organisaties van toepassing in vergelijking met de NIS1-richtlijn, waaronder mkb-bedrijven en bevat strenge beveiligingsplichten. De opdrachtgever wil daarom een checklist aanbieden, zodat mkb-bedrijven eenvoudig kunnen controleren of zij binnen het toepassingsbereik van de NIS2-richtlijn vallen en welke juridische verplichtingen daarbij komen kijken.

De vraag die in dit onderzoek centraal staat is:
'Welke ontwerpeisen zijn na een analyse van de wettelijke vereisten vanuit de NIS1-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen, de NIS2-richtlijn, praktijkervaringen met betrekking tot de huidige NIS1-richtlijn en praktijkervaringen met betrekking tot de aankomende NIS2-richtlijn en het testen van een concept checklist, toepasbaar op de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen?'

Om antwoord te geven op deze onderzoeksvraag is een theoretisch onderzoek en praktijkonderzoek uitgevoerd. Tijdens het theoretisch onderzoek zijn de vereisten van de NIS1-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen en de NIS2-richtlijn onderzocht. Daarnaast zijn de NIS1- richtlijn en de NIS2-richtlijn met elkaar vergeleken. Uit de theorie blijkt dat de checklist moet voldoen aan de juridische verplichtingen van de NIS2-richtlijn, zoals de beveiligingsplicht en de meldplicht. Daarnaast is het ook belangrijk om aan te tonen op welke organisaties de NIS2-richtlijn van toepassing is, zodat de organisaties weten of ze aan de verplichtingen van de richtlijn moeten voldoen.

Voor het praktijkonderzoek zijn interviews gehouden met verschillende organisaties. Daarnaast is de checklist van feedback voorzien en is deze getest. Tot slot is er voor het praktijkonderzoek een best practice bestudeerd. Voor het praktijkonderzoek zijn er verschillende organisaties geïnterviewd met betrekking tot de kennis en ervaringen met de huidige NIS1-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen en de nieuwe NIS2-richtlijn. Daarnaast is er ook met een toezichthouder van de Wet Beveiliging Netwerk- en Informatiesystemen gesproken die ook betrokken is bij de Nederlandse implementatie van de NIS2-richtlijn. Uit deze interviews zijn de kennis en ervaringen van zowel de NIS1-richtlijn en de NIS2-richtlijn van mkb-bedrijven in kaart gebracht. Daarnaast is het toezicht van de Wet Beveiliging Netwerk- en Informatiesystemen en de implementatie van de NIS2-richtlijn verwerkt in het onderzoek. Uit het praktijkonderzoek blijkt dat organisaties cybersecurity ontzettend belangrijk vinden en dit ook toe passen binnen de organisatie. Daarnaast blijkt dat de impact van de NIS2-richtlijn vooral groot kan zijn op organisaties met weinig tot geen juridische kennis en dat het lastig is om de genomen maatregelen aantoonbaar te maken.

Aan de hand van het theoretisch onderzoek, het praktijkonderzoek en meerdere gesprekken met de opdrachtgever is er een checklist tot stand gekomen. De checklist is van feedback voorzien door de drie organisaties waar ook een interview is afgenomen. Aan de hand van de feedback zijn er wijzigingen aangebracht in de checklist. Dezelfde drie organisaties hebben de checklist ook getest. De conclusie van het testen is dat de checklist overzichtelijk en gebruiksvriendelijk is. Ook willen de organisatie de checklist toepassen binnen de organisatie.

1. Inleiding

In hoofdstuk één wordt een inleiding gegeven over het afstudeeronderzoek. In paragraaf 1.1 wordt de opdrachtgever van het afstudeeronderzoek besproken. In paragraaf 1.2 de probleembeschrijving van het onderzoek. In paragraaf 1.3 wordt het beroepsproduct besproken met daarin de eisen waar het beroepsproduct aan moet voldoen. In paragraaf 1.4 wordt de onderzoekdoelstelling geformuleerd. In paragraaf 1.5 wordt de centrale onderzoeksvraag behandeld en tot slot in paragraaf 1.6 de theorie- en praktijkdeelvragen.

1.1 De opdrachtgever

Dit afstudeeronderzoek is uitgevoerd in opdracht van het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen. Het lectoraat onderzoekt complexe juridische vraagstukken die voor ondernemers relevant zijn.[1] Het doel van het lectoraat is om de wet- en regelgeving beter aan te laten sluiten op de behoeften van ondernemers.[2] De focus van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool richt zich op:

1. digitale transformatie;
2. impact ondernemerschap; en
3. governance.[3]

Het afstudeeronderzoek is een samenwerking met het project Cybersecurity Noord-Nederland. Het project Cybersecurity Noord-Nederland is een samenwerking met de Hanzehogeschool, RUG, TNO, Noorderpoort, Alfa college en andere partijen.[4] Om die samenwerking vast te leggen, is er in Groningen en in Friesland een stichting opgericht ter vergroting van de cyber weerbaarheid: de Stichting Cyber Safety Noord-Nederland in Friesland en de Stichting Security Centrum Noord- Nederland in Groningen. Bij beide stichtingen zijn samen ongeveer

1 ‘Juridische Aspecten van Ondernemerschap’, hanze.nl.
2 ‘Juridische Aspecten van Ondernemerschap’, hanze.nl.
3 ‘Juridische Aspecten van Ondernemerschap’, hanze.nl.
4 ‘Juridische Aspecten van Ondernemerschap’, hanze.nl.

zestig organisaties aangesloten. De stichtingen vormen samen Cyber Security Noord. De bedoeling is dat dit centrum uitgroeit tot een van de belangrijkste landelijke expertisecentra op het gebied van cybersecurity en daarmee een actieve bijdrage levert aan de Nederlandse cybersecurity agenda.[5]

Het project heeft onder andere tot doel om onderzoek en kennisontwikkeling op het gebied van cybersecurity te versnellen en zichtbaar te laten zijn. Daarnaast heeft het project als doel om de weerbaarheid van mkb-bedrijven te vergroten door middel van verbeterde kennis- en expertisedeling. Hierbij worden door studenten nieuwe producten en diensten ontwikkeld op het gebied van cybersecurity die door bedrijven gebruikt kunnen worden.[6]

De opdrachtgever is dr. T.R. Mulder. Haar functie is lector bij het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen. Dr. T.R. Mulder is jurist en in maart 2022 gepromoveerd aan de Rijksuniversiteit Groningen op privacy en gezondheidsgegevens. Daarnaast heeft dr. T.R. Mulder de afgelopen jaren gewerkt als senior coördinerend jurist bij de Ministeries van Binnenlandse Zaken en Koninkrijksrelaties en Volksgezondheid, Welzijn en Sport.

1.2 Probleembeschrijving

Met de groeiende digitalisering in onze maatschappij neemt ook het aantal cyberaanvallen toe. Er is dringende behoefte aan kennis op het gebied van cybersecurity. De aanleiding voor het onderzoek is de NIS2-richtlijn. NIS staat voor ‘Network And Information Security directive’, in het Nederlands ‘Netwerk- en Informatiesystemen’.[7]

Op 14 december 2022 is de NIS2-richtlijn door de Europese Unie aangenomen, welke uiterlijk op 17 oktober 2024 moet zijn geïmplementeerd door de lidstaten van de Europese Unie.[8] De afgelopen jaren zijn er verschillende ontwikkelingen op het gebied van cyberrisico’s die de veiligheid van onze maatschappij en economie steeds meer onder druk zetten. De komst van de NIS2-richtlijn moet bijdragen aan meer Europese harmonisatie van cybersecurity en een hoger niveau van cybersecurity bij organisaties.[9] De implementatie van de NIS2-richtlijn is omvangrijk en een complex traject. De NIS2-richtlijn is voor meer organisaties van toepassing en brengt meer verplichtingen met zich mee. Daarom is het belangrijk om te onderzoeken wat de vereisten van de richtlijn zijn en hoe mkb- bedrijven hier in de praktijk uitvoering aan kunnen geven. Organisaties weten aan de hand van het beroepsproduct wanneer zij als organisatie moeten voldoen aan de NIS2-richtlijn en welke verplichtingen daaruit voortvloeien. Zo kunnen organisaties zich voorbereiden op de nieuwe NIS2- richtlijn en werken aan een betere cyberweerbaarheid.

5 ‘Noord-Nederland beter beschermd tegen cyberaanvallen’, cybersecurity-noord.nl.
6 ‘Cybersecurity Noord-Nederland: Kennis- ontwikkeling versnellen en zichtbaar maken’, hanze.nl.
7 ‘NIS2-richtlijn’, digitaleoverheid.nl.
8 ‘Wat gaat de NIS2-richtljn betekenen voor uw organisatie?’, ncsc.nl.
9 ‘NIS2-richtlijn’, digitaleoverheid.nl.

1.3 Beroepsproduct

Naast het onderzoeksrapport wordt ook een beroepsproduct gemaakt in de vorm van een checklist. Deze wordt vanuit het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen aangeboden aan mkb-bedrijven. De checklist is daarnaast ook voor andere organisaties van toepassing aangezien de informatie in de checklist ook voor hen relevant is. De checklist wordt aangeboden op een (digitale) flyer met informatie op de voor- en achterkant. Op de voorkant van de checklist kunnen organisaties erachter komen of zij binnen het toepassingsbereik van de NIS2-richtlijn vallen. Op de checklist worden een aantal vragen gesteld die de organisatie stapsgewijs kan volgen. Zo weet de organisatie of ze wel of niet binnen het toepassingsbereik van de NIS2-richtlijn vallen en of ze aan de verplichtingen van deze richtlijn moeten voldoen. Op de achterkant van de checklist staan de beveiligingseisen van de NIS2-richtlijn. Ook wordt er via een QR-code verwezen naar een pagina waar extra informatie over deze beveiligingseisen te vinden is.

De checklist levert een bijdrage voor organisaties die op dit moment al binnen het toepassingsbereik van de Wet Beveiliging Netwerk- en Informatiesystemen vallen en met behulp van de checklist kunnen zien welke extra stappen zij moeten ondernemen om ook aan de NIS2-richtlijn te voldoen. Daarnaast levert de checklist ook een bijdrage voor mkb-bedrijven die in de toekomst aan de eisen van de NIS2-richtlijn moeten voldoen en voor andere organisaties die willen weten of ze überhaupt binnen het toepassingsbereik van de NIS2-richtlijn vallen.

De checklist moet aan de volgende eisen voldoen:

- de checklist moet overzichtelijk en gebruiksvriendelijk zijn;
- de checklist moet eenvoudig te lezen zijn voor organisaties, ook voor organisaties met weinig tot geen juridische kennis;
- de huisstijl van de checklist moet in de kleuren van het Lectoraat Juridische Aspecten van Ondernemerschap, daarnaast moet het logo van Cybersecurity Noord-Nederland op de checklist staan;
- op de voorkant van de checklist moeten organisaties erachter kunnen komen of de organisatie binnen het toepassingsbereik van de NIS2-richtlijn valt. Hier kunnen organisaties achter komen door een aantal vragen te beantwoorden. Het gaat om de volgende vragen: de vraag in welke sector de organisatie zich bevindt, de vraag of de organisatie in Nederland is gevestigd, de vraag hoeveel medewerkers een organisatie in dienst heeft en de vraag of een organisatie een jaaromzet en balanstotaal van meer dan tien miljoen heeft;
- op de voorkant van de checklist staat een QR-code die verwijst naar de zelf-evaluatie van de Rijksoverheid. Aan de hand van de zelf-evaluatie kunnen organisaties er ook achter komen of ze wel of niet binnen het toepassingsbereik van de NIS2-richtlijn vallen. Daarnaast wordt er via de zelf-evaluatie extra informatie gegeven over onder andere de sectoren en eventuele uitzonderingen;
- op de achterkant van de checklist staan de beveiligingseisen van de NIS2-richtlijn. De beveiligingseis wordt op de checklist kort omschreven. Aan de hand van de checklist kunnen organisaties per beveiligingseis afvinken of ze aan de verplichting voldoen; en

- op de achterkant van de checklist staat een QR-code die verwijst naar een pagina met meer informatie over de beveiligingseisen. Daar worden de beveiligingseisen uitgebreider toegelicht en worden ook andere onderdelen van de NIS2-richtlijn, zoals de meldplicht en toezicht, besproken.

1.4 Onderzoeksdoelstelling

Het doel van dit onderzoek is het opleveren van een checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen, dat is gebaseerd op de (toepassings)vereisten van de NIS1-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen en de NIS2-richtlijn zijn, rekening houden met kennis en ervaringen uit praktijk met betrekking tot de uitvoering van de NIS1-richtlijn, kennis en ervaringen uit de praktijk met betrekking tot de voorbereiding van de NIS2-richtlijn, en is afgestemd op het testen van een concept van de checklist.

1.5 Centrale onderzoeksvraag

De centrale onderzoeksvraag van dit onderzoek is:

'Welke ontwerpeisen zijn na een analyse van de wettelijke vereisten vanuit de NIS1-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen, de NIS2-richtlijn, praktijkervaringen met betrekking tot de huidige NIS1-richtlijn en praktijkervaringen met betrekking tot de aankomende NIS2-richtlijn en het testen van een concept checklist, toepasbaar op de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen?'

1.6 Deelvragen

De centrale onderzoeksvraag wordt aan de hand van een aantal theorie- en praktijkdeelvragen beantwoord.

1.6.1 Theoriedeelvragen

De theoriedeelvragen van dit onderzoek zijn:

1. Welke ontwerpeisen voor de checklist voor het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit de toepasselijke wetsartikelen uit de NIS1-richtlijn?
2. Welke ontwerpeisen voor de checklist voor het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit de verschillen en overeenkomsten tussen de NIS1-richtlijn en de Wet Beveiliging Netwerk- en Informatiesystemen?
3. Welke ontwerpeisen voor de checklist voor het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit de toepasselijke wetsartikelen uit de NIS2-richtlijn?
4. Welke ontwerpeisen voor de checklist voor het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit de verschillen tussen de NIS1-richtlijn en de NIS2-richtlijn?

1.6.2 Praktijkdeelvragen

De praktijkdeelvragen van dit onderzoek zijn:

1. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen zijn af te leiden uit de kennis en ervaring van mkb-bedrijven met betrekking tot de uitvoering van de huidige NIS1-richtlijn?
2. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen zijn af te leiden uit de kennis en ervaring van mkb-bedrijven met betrekking tot de voorbereiding van de NIS2-richtlijn?
3. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen zijn af te leiden uit de kennis van de toezichthouders van de Wet Beveiliging Netwerk- en Informatiesystemen?
4. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen zijn af te leiden uit de NIS2 zelfevaluatie NL dat ontwikkeld is door de Rijksoverheid?
5. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit het testen van een concept checklist door medewerkers van de mkb-bedrijven?

2. Methodologische verantwoording

In hoofdstuk 2 worden de methoden besproken die zijn toegepast om de centrale onderzoeksvraag te beantwoorden. In paragraaf 2.1 worden de bronnen besproken die zijn gebruikt voor het theoretisch onderzoek, zoals de wet- en regelgeving en de literatuur. in paragraaf 2.2 worden de onderzoeksmethoden besproken die zijn gebruikt voor het praktijkonderzoek, de beste practice en het testpaneel van het beroepsproduct. Tot slot wordt in paragraaf 2.3 de kwaliteiten en beperkingen van dit onderzoek besproken.

2.1 Theoretische bronnen

Om de theoretische onderzoeksvragen uit dit onderzoek te kunnen beantwoorden, is er gebruik gemaakt van wet- en regelgeving en juridische literatuur. Hieronder wordt toegelicht welke wet- en regelgeving is toegepast, welke andere bronnen er zijn gebruikt en waarom deze bronnen zijn gekozen.

2.1.1 Wet- en regelgeving

Om de theoriedeelvragen te beantwoorden zijn er verschillende wet- en regelgeving geraadpleegd. De belangrijkste bronnen voor dit onderzoek zijn de NIS1-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen, het Besluit Beveiliging Netwerk- en Informatiesystemen en de NIS2-richtlijn. Daarnaast zijn ook samenvattingen van beide richtlijn via EUR-lex geraadpleegd. De wettekst van de NIS1-richtlijn is geraadpleegd om te achterhalen op welke organisaties de NIS1-richtlijn van toepassing is en wat de verplichtingen van deze richtlijn zijn. De NIS1-richtlijn is in Nederland geïmplementeerd in de Wet Beveiliging Netwerk- en Informatiesystemen en is op dit moment in werking. De wettekst van de Wet Beveiliging Netwerk- en Informatiesystemen en het Besluit Beveiliging Netwerk- en Informatiesystemen zijn geraadpleegd om de NIS1-richtlijn te vergelijken in de verschillen en overeenkomsten met de Nederlandse implementatie daarvan. Naast de wettekst van de huidige NIS1-richtlijn is ook de wettekst van de aankomende NIS2-richtlijn geraadpleegd. De wettekst van de NIS2-richtlijn is geraadpleegd om erachter te komen op wie de NIS2-richtlijn van toepassing is en welke verplichtingen de richtlijn met zich mee brengt. Daarnaast is de wettekst van de NIS2-richtlijn geraadpleegd om beide richtlijnen met elkaar te vergelijken.

De Algemene Verordening Gegevensbescherming, Verordening (EG) nr. 45/2001, wordt niet behandeld in dit onderzoek. De Algemene Verordening Gegevensbescherming heeft ook bepaalde beveiligingseisen, maar een onderzoek naar de Algemene Verordening Gegevensbescherming is een onderzoek op zichzelf gezien de hoeveelheid wettekst van de verordening. Ongeacht de verwachting dat de Algemene Verordening Gegevensbescherming van toepassing is op iedere organisatie die aan de vereisten NIS2-richtlijn moet voldoen. Dit komt omdat de wet- en regelgeving van de Algemene Verordening Gegevensbescherming los staat van de NIS2-richtlijn. Organisaties kunnen er niet automatisch van uit gaan dat als zij aan de verplichtingen van de Algemene Verordening Gegevensbescherming voldoen, ook aan de verplichtingen van de NIS2-richtlijn voldoen. De organisaties moeten van geval tot geval beoordelen welke beveiligingsstappen zij specifiek onder beide wetten moeten hanteren. De Algemene Verordening Gegevensbescherming wordt daarom niet meegenomen in dit onderzoek. Er wordt in dit onderzoek gefocust op de NIS1-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen, het Besluit Beveiliging Netwerk- en Informatiesystemen en de NIS2-richtlijn.

2.1.2 Handboeken

Naast de wet- en regelgeving is er ook een handboek geraadpleegd, namelijk: ‘De grondslagen van de cyberspace’ van A.G. Awesta. In dit handboek wordt de achtergrond informatie van de beveiliging van netwerk- en informatiesystemen behandeld. Daarnaast wordt ook het traject van de implementatie van de richtlijn, het toepassingsbereik en de uitvoering van de NIS1-richtlijn behandeld. Dit handboek is geraadpleegd om kennis op te doen over de huidige NIS1-richtlijn en het implementatietraject.

Daarnaast is het handboek geraadpleegd om het toepassingsbereik van de NIS1-richtlijn in kaart te brengen. In dit onderzoek is er geen handboek over de NIS2-richtlijn geraadpleegd aangezien de NIS2-richtlijn een nieuwe richtlijn is en er nog geen handboeken over deze richtlijn zijn.

2.1.3 Juridische tijdschriften

Ook is in dit onderzoek gebruik gemaakt van artikelen uit juridische tijdschriften, zoals het tijdschrift ‘Nederlands Juristenblad’ en het tijdschrift ‘Computerrecht’. Zo is het artikel ‘Cybersecurity in Europa’ van N. Brouwer en J. van Mil van het Nederlands Juristenblad geraadpleegd om inzicht te krijgen in de verschillen en overeenkomsten van de NIS1-richtlijn, de Wet beveiliging Netwerk- en Informatie Systemen en de NIS2-richtlijn. Deze bron behandeld de belangrijkste elementen uit de wet- en regelgeving en formuleert dit overzichtelijk in een artikel. Daarnaast is het artikel ‘Cybersecuritywet’ van het Nederlands Juristenblad gebruikt om inzicht te krijgen in de NIS1-richtlijn. In het artikel worden alle belangrijke elementen van de NIS1-richtlijn genoemd, zoals de reikwijdte, de beveiligingseisen, de meldplicht, toezicht en sancties van de NIS1-richtlijn. Ook is het artikel ‘de NIS2- richtlijn’ van T. Wondolleck en E. ’t Hart van het Nederlands Juristenblad geraadpleegd om inzicht te krijgen in de achtergrond, de verplichtingen, de governance en de voorbereiding op de NIS2-richtlijn.

2.1.4 Online bronnen

Tot slot zijn er ook online bronnen geraadpleegd van verschillende overheidsorganisaties, zoals: de Rijksoverheid, het Nationaal Cyber Security Centrum, het Nationaal Coördinator Terrorismebestrijding en Veiligheid en de Rijksinspectie Digitale Infrastructuur. Deze bronnen gaven onder andere inzicht in hoe en wanneer de NIS2-richtlijn in Nederland wordt geïmplementeerd en wat de tijdlijn van de NIS2-richtlijn is. Daarnaast wordt ook het doel van de NIS-richtlijnen, het toepassingsbereik en de verplichtingen behandeld. Door deze literatuur te raadplegen is het mogelijk om in kaart te brengen wat de belangrijkste elementen uit de NIS-richtlijnen zijn.

2.2 Onderzoeksmethoden en- objecten

Voor het praktijkonderzoek zijn verschillende onderzoeksmethoden en- objecten toegepast. Ten eerste zijn er verschillende interviews afgenomen bij verschillende organisaties. De interviews zijn van belang voor het onderzoek om erachter te komen wat de kennis en ervaringen zijn met betrekking tot de huidige Wet Beveiliging Netwerk- en Informatiesystemen. Daarnaast wordt er aan de hand van de interviews in kaart gebracht wat de kennis en ervaringen zijn van organisaties met betrekking tot de nieuwe NIS2-richtlijn. Er is voor de onderzoeksmethode ‘interview’ gekozen omdat, in tegenstelling tot bij een enquête, kan worden doorgevraagd.

2.2.1 Onderzoeksmethoden

Voor dit onderzoek is de onderzoeksmethode ‘interview’ gebruikt. Hier is voor gekozen, omdat er tijdens een interview de mogelijkheid is om door te vragen op bepaalde antwoorden. Zo kan zoveel mogelijk informatie uit een gesprek worden gehaald. De verschillende organisaties en het gesprek met de toezichthouder spelen een belangrijke rol in het onderzoek. Daarom is het belangrijk om door de interviewmethode inzicht te krijgen in onder andere de mening, overtuigingen en werkwijze van deze organisaties. Daarnaast is op het beroepsproduct feedback gegeven en is het beroepsproduct getest.

2.2.2 Onderzoeksobjecten

Er zijn in totaal drie verschillende organisaties geïnterviewd die te maken (gaan) hebben met de NIS- richtlijnen en één toezichthoudende overheidsorganisatie. Voor alle organisaties is een aparte interviewvragenlijst gemaakt aangezien de organisaties allemaal op een andere manier met de NIS- richtlijnen te maken hebben.

Ten eerste is een overheidsorganisatie geïnterviewd die op dit moment al binnen het toepassingsbereik van de Wet Beveiliging Netwerk- en Informatiesystemen valt. De overheidsorganisatie is gevestigd in Groningen en levert drinkwater in de provincie Groningen en voor een deel in de provincie Drenthe. Binnen de Wet Beveiliging Netwerk- en Informatiesystemen valt de organisatie onder de (vitale) sector ‘levering en distributie van drinkwater’. Voor deze overheidsorganisatie is gekozen aangezien zij op dit moment al de eisen van de Wet Beveiliging Netwerk- en Informatiesystemen hanteren. De overheidsorganisatie kan veel informatie geven over de uitvoering van de Wet Beveiliging Netwerk- en Informatiesystemen, maar ook bijvoorbeeld over hoe het toezicht eruit ziet. In bijlage 6 staat de interviewvragenlijst.

Ten tweede is een organisatie geïnterviewd die op dit moment niet binnen het toepassingsbereik van de Wet Beveiliging Netwerk- en Informatiesystemen valt aangezien de organisatie minder dan één miljoen eindgebruikers heeft. Wel heeft de organisatie een ISO27001-certificaat in bezit waarin ook beveiligingseisen voor netwerk- en informatiesystemen staan. De organisatie is gevestigd in Groningen en biedt telefonie aan in de Cloud voor bedrijven. De organisatie valt op dit moment niet binnen het toepassingsbereik van de Wet Beveiliging Netwerk- en Informatiesystemen, maar wel binnen het toepassingsbereik van de toekomstige NIS2-richtlijn. Voor deze organisatie is gekozen aangezien zij op dit moment nog niet aan de eisen van de Wet Beveiliging Netwerk- en Informatiesystemen hoeven te voldoen, maar in de toekomst wel aan de NIS2-richtlijn. Het is daarom waardevol om erachter te komen hoe een organisatie zich op de komst van de NIS2-richtlijn voorbereid. Daarnaast hanteert de organisatie wel de ISO 27001 en is de organisatie daarom op de hoogte wat voor impact de beveiligingseisen op een organisatie kan hebben. In bijlage 7 staat de interviewvragenlijst.

Ten derde is een organisatie geïnterviewd die op dit moment nog niet in aanmerking komt voor de NIS2-richtlijn, maar gezien de groei van de organisatie waarschijnlijk in de toekomst wel. De organisatie is gevestigd in Groningen en biedt software op het gebied van debiteurenbeheer. De organisatie is goed op de hoogte van beveiliging van netwerk- en informatiesystemen en is inmiddels acht jaar ISO27001-gecertificeerd. Voor deze organisatie is gekozen aangezien zij op dit moment nog niet binnen het toepassingsbereik van de NIS2-richtlijn vallen, maar waarschijnlijk in de toekomst wel. Het is waardevol om erachter te komen in hoeverre dit soort organisaties bekend zijn met de NIS2-richtlijn en hoe zij zich, gericht op de toekomst, hier op voorbereiden. In bijlage 8 staat de interviewvragenlijst.

Ten vierde is een overheidsorganisatie geïnterviewd die toezichthouder is op de Wet Beveiliging Netwerk- en Informatiesystemen. Daarnaast is de overheidsorganisatie ook betrokken bij de totstandkoming van de NIS2-richtlijn en de implementatie van de richtlijn. De overheidsorganisatie is gevestigd in Groningen en Amersfoort en is toezichthouder op het gebied van telecommunicatie en IT-netwerken in Nederland. Voor deze overheidsorganisatie is gekozen aangezien zij toezicht houden op de naleving van de Wet Beveiliging Netwerk- en Informatiesystemen. Daarnaast is de organisatie betrokken bij de totstandkoming en implementatie van de NIS2-richtlijn. Het is waardevol om de verwachtingen van de Nederlandse implementatie van de NIS2-richtlijn mee te nemen in het onderzoek. In bijlage 9 staat de interviewvragenlijst.

Tot slot is feedback gegeven op het beroepsproduct en is het beroepsproduct getest door de drie organisaties die ook zijn geïnterviewd en te maken (gaan) hebben met de NIS-richtlijnen. Naast de feedback van de organisaties die zijn geïnterviewd is ook de feedback van de opdrachtgever verwerkt in de definitieve versie van het beroepsproduct. Er is voor deze drie organisatie gekozen aangezien zij aan de beveiligingseisen van de NIS2-richtlijn moeten voldoen. Daarnaast is het voor de organisaties van belang om te controleren of ze binnen het toepassingsbereik van de NIS2-richtlijn vallen. De beveiligingseisen en het toepassingsbereik komen beide in het beroepsproduct terug. Tijdens de interviews is om feedback gevraagd op de checklist. De feedback is vervolgens verwerkt in een nieuwe versie van de checklist en is vervolgens getest door dezelfde drie organisaties. Naar aanleiding van het testen zijn de laatste definitieve aanpassingen gedaan. In bijlage 11 en 12 staan de eerste twee versies van het beroepsproduct en in bijlage 13 de definitieve versie.

2.2.3 Meetinstrumenten en verwerking resultaten

Het meetinstrument dat is gebruikt binnen het praktijkonderzoek is een interviewvragenlijst. De interviews hebben één-op-één plaatsgevonden waardoor er gedetailleerde informatie is verkregen. Bij alle interviews is voor een deels gestructureerd interview gekozen. In een gestructureerd interview zijn de formulering en de volgorde van de vragen vastgelegd. Op basis van de antwoorden tijdens het interview is er op bepaalde onderwerpen doorgevraagd. De interviews zijn volledig uitgeschreven en de waardevolle uitkomsten zijn opgenomen in het onderzoek.

2.2.4 Best practices

De best practice die is bestudeerd voor het onderzoek is een zelf-evaluatie van de NIS2-richtlijn van de Rijksoverheid. Aan de hand van de zelf-evaluatie kunnen organisaties erachter komen of zij binnen het toepassingsbereik van de NIS2-richtlijn vallen. Er zijn verschillende rondes zoals het bepalen van de sector en het bepalen van de grote van de organisatie. Per ronde kan een organisatie verder klikken met uiteindelijk het resultaat of de organisatie wel of niet binnen het toepassingsbereik van de NIS2-richtlijn valt. De zelfevaluatie was representatief voor de voorkant van de checklist aangezien daar het toepassingsbereik van de NIS2-richtlijn wordt omschreven. Op de checklist wordt via een QR-code verwezen naar de zelf-evaluatie van de Rijksoverheid. Er is namelijk via de checklist niet de mogelijkheid om door te klikken en dit kan via de zelfevaluatie van de Rijksoverheid wel. In bijlage 10 staat de zelf-evaluatie van de Rijksoverheid.

2.2.5 Definitieve ontwerpeisen

De inhoud van de checklist is tot stand gekomen door het theorie- en praktijkonderzoek en zijn verwerkt in de checklist. Aan de hand van het theoretisch onderzoek is er bepaald welke ontwerpeisen uit de richtlijn worden meegenomen in de checklist. De ontwerpeisen uit het praktijkonderzoek zien met name op de uitvoering van de huidige Wet Beveiliging Netwerk- en Informatiesystemen en de verwachtingen van de uitvoering van de NIS2-richtlijn. Niet alle ontwerpeisen zijn verwerkt in de checklist aangezien dit te veel ontwerpeisen zijn om in een checklist te verwerken. De afweging voor de ontwerpeisen die in dit onderzoek zijn gemaakt, is of de informatie van toegevoegde waarde is voor de organisaties. De belangrijkste informatie zoals het toepassingsbereik, de beveiligingseisen en de meldplicht zijn opgenomen in het beroepsproduct. Daarnaast is ervoor gekozen om met behulp van een QR-code naar een webpagina met meer informatie te verwijzen. In bijlage 14 staat de extra informatie waar naar wordt verwezen in de checklist.

2.3 Kwaliteiten en beperkingen

In deze paragraaf worden de kwaliteiten en beperkingen van dit onderzoek besproken. In paragraaf worden de kwaliteiten besproken en in paragraaf 2.6.1 de beperkingen.

De lengte van dit onderzoek is geen kwaliteit en geen beperking. De lengte van het onderzoeksrapport heeft mij in staat gesteld om elke deelvraag grondig te onderzoeken,

waardoor een volledig begrip van zowel de theoretische en praktische aspecten van het onderwerp mogelijk is geworden. Daarnaast is de informatie die in dit onderzoeksrapport wordt behandeld zorgvuldig uitgekozen. Elke deelvraag heeft een bijdrage geleverd aan het onderzoek. Kortom, hoewel de lengte van dit onderzoek afwijkt van de gangbare richtlijn, is deze lengte gerechtvaardigd om de theorie- en praktijkdeelvragen grondig te behandelen en om nieuwe inzichten te kunnen bieden.

2.3.1 Kwaliteiten

De kwaliteit van het onderzoek is de actualiteit van het onderwerp, de NIS-richtlijnen. Over zowel de NIS1-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen en de NIS2-richtlijn is veel informatie te vinden. Daarnaast wordt er over de NIS2-richtlijn steeds nieuwe literatuur gepubliceerd. Daardoor was er voor dit onderzoek genoeg informatie te vinden. De literatuur die is toegepast in dit onderzoek is zorgvuldig uitgekozen.

Daarnaast is een kwaliteit van dit onderzoek de verschillende interviews die hebben plaatsgevonden. Zo zijn er verschillende kandidaten gesproken van verschillende organisaties die allemaal op een andere manier te maken hebben of gaan krijgen met de NIS-richtlijnen. Daarnaast heeft er ook een interview plaatsgevonden met een toezichthoudende organisatie van de Wet Beveiliging Netwerk- en Informatiesystemen die ook betrokken is bij de implementatie van de NIS2-richtlijn. Hierdoor ontstond een goed beeld van de huidige Wet Beveiliging Netwerk- en Informatiesystemen en de verwachtingen van de toekomstige NIS2-richtlijn. Dit veelzijdige beeld is meegenomen in de ontwerpeisen van de checklist.

Een kwaliteit van dit onderzoek is dat het beroepsproduct voor zowel mkb-bedrijven en voor andere organisaties van toepassing kan zijn. Daarnaast is het beroepsproduct veelzijdig aangezien het toepassingsbereik en de verplichtingen van de NIS2-richtlijn erin worden verwerkt. Ook kunnen organisaties met behulp van de QR-code extra informatie krijgen over de verplichtingen van de NIS2- richtlijn. Hierbij wordt er rekening gehouden met de schrijfstijl van de teksten, zodat het ook voor organisaties met geen of weinig juridische kennis duidelijk is. Daarnaast is het beroepsproduct meerdere malen van feedback voorzien en getest door verschillende organisaties. Daardoor is het duidelijk dat het beroepsproduct gebruiksvriendelijk is en dat organisaties het beroepsproduct in de praktijk willen raadplegen.

2.3.2 Beperkingen

Een beperking van het onderzoek is dat er geen organisatie is gesproken die wel in aanmerking gaat komen voor de NIS2-richtlijn, maar geen ISO27001-certificaat heeft. Tijdens het benaderen van kandidaten voor het praktijkonderzoek was het lastig om kandidaten te vinden die de NIS1-richtlijn nog niet hanteren, wel de NIS2-richtlijn moeten gaan hanteren en geen ISO27001-certificaat hebben. Er zijn verschillende organisaties benaderd, maar deze organisaties hebben geen reactie gegeven of stonden niet open voor een interview. Uiteindelijk is ervoor gekozen om een organisatie te interviewen die wel in het bezit is van een ISO27001-certficaat en waarschijnlijk in de toekomst aan de NIS2-richtlijn moet gaan voldoen. De beperking hierbij is dat het lastig is om in te schatten wat de impact gaat zijn van de NIS2-richtlijn voor een organisatie die op dit moment nog niet in het bezit is van een ISO27001-certificaat. Voor ISO27001 moeten er namelijk ook worden voldaan aan bepaalde beveiligingseisen voor netwerk- en informatiesystemen. Anderzijds hebben de andere interviews waardevolle informatie opgeleverd, waardoor er toch een goed beeld is gegeven van de kennis en ervaringen van de NIS2-richtlijn. De enige beperking hierin is dat een organisatie zonder ISO27001- certificaat dit niet kan bevestigen.

2.3.3 Conclusie waarde onderzoek

Dankzij de resultaten van het onderzoek is er een checklist tot stand gekomen. Ondanks dat niet de gewenste kandidaat is geïnterviewd, hebben de andere kandidaten een positieve bijdrage geleverd aan het onderzoek. Dankzij de informatie vanuit de wet- en regelgeving, de interviews, best practice, en het testpaneel van het beroepsproduct is er een checklist tot stand gekomen. Aan de hand van de checklist kunnen organisaties erachter komen of ze vallen onder het toepassingsbereik van de NIS2- richtlijn. Daarnaast kunnen de organisaties contoleren wat de vereisten van de NIS2-richtlijn zijn en welke stappen de organisatie nog moet ondernemen om aan de eisen van de NIS2-richtlijn te voldoen.

3. Ontwerpeisen vanuit de theorie

In hoofdstuk drie worden de resultaten van het theoretisch onderzoek besproken. Dit wordt gedaan aan de hand van de volgende deelvragen:

1. Welke ontwerpeisen voor de checklist voor het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit de toepasselijke wetsartikelen uit de NIS1-richtlijn?
2. Welke ontwerpeisen voor de checklist voor het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit de verschillen en overeenkomsten tussen de NIS1-richtlijn en de Wet Beveiliging Netwerk- en Informatiesystemen?
3. Welke ontwerpeisen voor de checklist voor het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit de toepasselijke wetsartikelen uit de NIS2-richtlijn?
4. Welke ontwerpeisen voor de checklist voor het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit de verschillen tussen de NIS1-richtlijn en de NIS2-richtlijn?

3.1 Ontwerpeisen wetsartikelen NIS1-richtlijn

De richtlijn 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, hierna de NIS1-richtlijn genoemd, is de eerste richtlijn om de cybersecurity in de Europese Unie te verbeteren en om eenheid te brengen in het Europese beleid voor netwerk- en informatiebeveiliging.[10] Een richtlijn is een rechtshandeling die een bepaald doel vastlegt die de landen van de Europese Unie moeten bereiken. Dit mogen de landen van de Europese Unie doen door zelf wetgeving vast te stellen om het doel van de richtlijn te bereiken.[11] De NIS1-richtlijn werd aangenomen op 6 juli 2016.

10 Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194)

11 ‘Soorten rechtshandelingen’, european-union.europa.eu.

De landen van de Europese Unie hebben de NIS1-richtlijn voor 9 mei 2018 geïmplementeerd in nationale wetgeving.[12] In Nederland is de NIS1-richtlijn geïmplementeerd in de Wet Beveiliging Netwerk- en Informatiesystemen.[13]

Om in kaart te brengen wat de toepasselijke wetsartikelen zijn van de NIS1-richtlijn worden de volgende onderwerpen besproken: het toepassingsbereik in paragraaf 3.1.2, de bevoegde autoriteiten in paragraaf 3.1.3, het CSIRT's in paragraaf 3.1.3, de beveiligingseisen in paragraaf 3.1.4, de meldplicht in paragraaf 3.1.7 en het toezicht, de handhaving en de sancties van de richtlijn in paragraaf 3.1.8.

3.1.1 Inleiding en begrip/definitie NIS1-richtlijn

Het doel van de NIS1-richtlijn is om een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de landen binnen de Europese Unie tot stand te brengen.[14] Hiermee wordt bedoeld de verbetering van het veiligheidsniveau van netwerk- en informatiesystemen en om diensten te beveiligen die cruciaal zijn voor de economie en samenleving in de Europese Unie. De lidstaten van de Europese Unie moeten op grond van artikel 7 uit de NIS1-richtlijn een strategie voor nationale cyberbeveiliging opzetten voor netwerk- en informatiesystemen.15 In bijlage 1 staat de nationale strategie. Daarnaast zijn in de richtlijn maatregelen voorgesteld ter verhoging van het veiligheidsniveau van netwerk- en informatiesystemen. De richtlijn heeft drie hoofddoelstellingen:

1. de nationale vermogens op het gebied van cyberbeveiliging verbeteren;
2. de samenwerking op niveau van de Europese Unie opbouwen; en
3. een cultuur van risicobeheer en melding van incidenten bevorderen bij belangrijke economische actoren.[16]

3.1.1.1 Het begrip 'cyberbeveiliging'

Het begrip 'cyberbeveiliging' betekent het vermogen van netwerk- en informatiesystemen om bestand te zijn tegen acties die de beschikbaarheid, vertrouwelijkheid, authenticiteit en integriteit van digitale gegevens of gerelateerde diensten die via de netwerk- en informatiesystemen worden aangeboden, in gevaar brengen.[17]

3.1.1.2 Het begrip 'netwerk- en informatiesystemen'

Onder 'netwerk- en informatiesystemen' wordt verstaan: "een elektronisch communicatienetwerk, of een apparaat of groep van onderling verbonden apparaten waarmee digitale gegevens worden verwerkt, alsmede de opgeslagen, verwerkte, opgehaalde of verzonden digitale gegevens".[18] De uitgebreide uitleg van netwerk- en informatiesystemen staat in artikel 2 van de NIS1-richtlijn.

12 'Samenvatting van Richtlijn EU 2016/1148 - Cyberbeveiliging van netwerk- en informatiesystemen', eur- lex.europa.eu.
13 'Wet Beveiliging netwerk- en informatiesystemen (Wbni)', rdi.nl.
14 Kalis 2017, p. 61.
15 'Samenvatting van Richtlijn EU 2016/1148 - Cyberbeveiliging van netwerk- en informatiesystemen', eur- lex.europa.eu.
16 Samenvatting van Richtlijn EU 2016/1148 - Cyberbeveiliging van netwerk- en informatiesystemen', eur- lex.europa.eu.
17 Samenvatting van Richtlijn EU 2016/1148 - Cyberbeveiliging van netwerk- en informatiesystemen', eur- lex.europa.eu.
18 'Samenvatting van Richtlijn EU 2016/1148 - Cyberbeveiliging van netwerk- en informatiesystemen', eur- lex.europa.eu.

3.1.2 Toepassingsbereik NIS1-richtlijn

De NIS1-richtlijn is van toepassing op aanbieders van essentiële diensten, digitale dienstverleners en overheidsorganisaties die essentiële diensten aanbieden.[19] Op 9 november 2018 zijn de aanbieders van essentiële diensten aangewezen.[20] De richtlijn laat de lidstaten van de Europese Unie vrij om regels te stellen over cybersecurity voor sectoren die in eerste instantie niet onder de richtlijn vallen.[21]

De richtlijn geeft drie criteria voor de identificatie van aanbieders van essentiële diensten:

1. de entiteit verleent een dienst die van essentieel belang is voor de instandhouding van kritieke maatschappelijke en/of economische activiteiten;
2. de verlening van die dienst is afhankelijk van netwerk- en informatiesystemen; en
3. een incident zou aanzienlijke verstorende effecten hebben voor de verlening van die dienst.[22]

De NIS1-richtlijn is van toepassing op aanbieders van essentiële diensten in van zeven sectoren:

1. bankwezen;
2. digitale infrastructuur;
3. energie;
4. gezondheidszorg;
5. infrastructuur voor de financiële markt;
6. levering en distributie van drinkwater; en
7. vervoer.[23]

3.1.3 Bevoegde autoriteiten

Om te beoordelen of de richtlijn goed wordt toegepast, wordt de richtlijn gemonitord door de nationale bevoegde autoriteiten. Elke lidstaat van de Europese Unie wijst één of meer nationale bevoegde autoriteiten aan voor de beveiliging van netwerk- en informatiesystemen.[24] Dit moeten de nationale bevoegde autoriteiten doen aan de hand van:

1. een beoordeling van de cyberbeveiliging en het beveiligingsbeleid van aanbieders van essentiële diensten op nationaal niveau;
2. door toezicht te houden op digitale dienstverleners
3. door deelname aan het werk van de samenwerkingsgroep. De samenwerkingsgroep bestaat uit de bevoegde autoriteiten op het gebied van netwerk- en informatiebeveiliging uit elk land van de Europese Unie, het Agentschap van de Europese Unie voor netwerk- en informatiebeveiliging (Enisa) en de Europese Commissie;
4. door, indien van toepassing, publiek te informeren om incidenten te voorkomen of om te gaan met een afzonderlijk incident; en
5. door het geven van bindende aanwijzingen om tekortkomingen op het gebied van cyberbeveiliging te verbeteren.[25]

19 'Cybersecuritywet', *NJB* 2018/480.
20 Art. 4 lid 4 van Richtlijn 2016/1148/EG.
21 'Cybersecuritywet', *NJB* 2018/480.
22 Art. 5 lid 2 Richtlijn 2016/1148/EG.
23 Art. 2 bijlage 2 Richtlijn 2016/1148/EG.
24 Art. 8 Richtlijn 2016/1148/EG.
25 'Samenvatting van Richtlijn EU 2016/1148 - Cyberbeveiliging van netwerk- en informatiesystemen', eur- lex.europa.eu.

3.1.4 Computer Security Incident Response Team (CSIRT's)

In Nederland is de Minister van Justitie en Veiligheid het centrale contactpunt voor aanbieders van een essentiële dienst, hierna het CSIRT.[26] Het CSIRT wil zeggen: de instantie voor de behandeling van vrijwillige meldingen.[27] Deze instantie is verantwoordelijk voor het monitoren van, en reageren op, incidenten op het gebied van cyberbeveiliging. Daarnaast zijn ze verantwoordelijk voor vroegtijdige waarschuwingen, alarmmeldingen, aankondigen en verspreiding van informatie over risico's en incidenten. Ook zijn ze verantwoordelijk voor het reageren op incidenten, zorgen voor een risicoanalyse, incidentenanalyse en situatiekennis. Tot slot moeten ze deelnemen aan het CSIRT- netwerk en moeten samenwerken met de particuliere sector.[28] Om de samenwerking te stimuleren, moedigen de CSIRT's de vaststelling en het gebruik van gestandaardiseerde praktijken op de volgende twee gebieden aan: de procesvoering voor de behandeling van incidenten en risico's en de systemen voor de indeling van incidenten, informatie en risico's.[29]

3.1.5 Beveiligingseisen NIS1-richtlijn

De beveiligingsplicht van de NIS1-richtlijn is een open norm en staat in artikel 14 van de NIS1- richtlijn. In het artikel staat dat aanbieders van essentiële diensten passende en evenredige maatregelen moeten treffen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen. In artikel 16 lid 1 van de NIS1-richtlijn staat de beveiligingsplicht voor digitale dienstverleners. Voor digitale dienstverleners zijn er meer algemene handvatten waar rekening mee gehouden moet worden.[30] Zoals de beveiliging van systemen en voorzieningen, de behandeling van incidenten, het beheer van de bedrijfscontinuïteit, toezicht, controle en testen en naleving van de internationale normen.[31]

3.1.6 Meldplicht

In de NIS1-richtlijn is er sprake van een incident als er feitelijk een schadelijk effect is op de beveiliging van netwerk- en informatiesystemen.[32] De meldingsdrempel bij de NIS1-richtlijn is als het gaat om een incident met aanzienlijke gevolgen voor de continuïteit van de dienst. Dit wordt beoordeeld door het aantal gebruikers dat door de verstoring wordt getroffen, de omvang van het geografisch gebied en de duur van het incident.[33] Mocht de duur van het incident zeer beperkt zijn, dan hoeft de getroffen entiteit dit niet te melden. De lidstaten van de Europese Unie hebben een vastgestelde procedure voor de behandeling van meldingen.[34] In hoofdstuk 3.2.5 wordt verder toegelicht hoe dit in Nederland is geregeld.

26 Artikel I van de wet van 17 oktober 2018 houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen) (Stb. 2018, 387).
27 Art. 2 WBNI.
28 Bijlage 1 Richtlijn 2016/1148/EG.
29 Bijlage 1 Richtlijn 2016/1148/EG.
30 Brouwer & Van Mil 2023, par. 2.2.1.
31 Art. 16 lid 1 Richtlijn 2016/1148/EG.
32 Art. 4 sub 7 Richtlijn 2016/1148/EG.
33 Brouwer & Van Mil 2023, par. 2.2.1.
34 Art. 20 lid 2 Richtlijn 2016/1148/EG.

3.1.7 Toezicht, handhaving en sancties

Er moet toezicht worden gehouden op de naleving van de beveiligingsplichten en meldplichten. Waar nodig moet er handhavend worden opgetreden. De richtlijn is op grond van artikel 3 van de NIS1-richtlijn gericht op minimumharmonisatie, behalve voor softwaresystemen. Een minimumharmonisatie houdt in dat de lidstaten aanvullende regels kunnen stellen en/of onderwerpen uitgebreider kunnen schikken dan hoe het in de richtlijn staat.[35]

De lidstaten van de Europese Unie moeten zorgen dat de bevoegde autoriteiten de naleving van de NIS1-richtlijn kunnen beoordelen. De bevoegde autoriteiten moeten bepaalde informatie kunnen vorderen van de essentiële entiteiten en digitale aanbieders. Als er uit de informatie blijkt dat er nalevingsproblemen zijn, dan moeten de bevoegde autoriteiten maatregelen kunnen nemen. Maatregelen kunnen bindende aanwijzingen en/of het informeren van het publiek over het incident zijn.[36]

In de NIS1-richtlijn staan geen specifieke sancties opgenomen. De lidstaten van de Europese Unie maken voorschriften van sancties die van toepassing zijn op het niet naleven van de richtlijn. Ook moeten de lidstaten van de Europese Unie ervoor zorgen dat de sancties daadwerkelijk worden uitgevoerd. De sancties moeten evenredig, doeltreffend, en afschrikkend zijn.[37]

3.1.8 Conclusie ontwerpeisen

Concluderend zijn dit de ontwerpeisen voor de checklist van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen die voortvloeien uit de NIS1-richtlijn:

- Het doel van de NIS1-richtlijn is om een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de landen van de Europese Unie tot stand te brengen. Hieruit vloeit de eerste ontwerpeis, namelijk: het doel van de NIS1-richtlijn moet duidelijk worden omschreven in de checklist, zodat organisaties weten waarom de NIS1-richtlijn er is.
- De NIS1-richtlijn is van toepassing op aanbieders van essentiële diensten die vallen onder één van de zeven sectoren die de NIS1-richtlijn voorschrijft en op digitale aanbieders. Hieruit vloeit de tweede ontwerpeis, namelijk: het toepassingsbereik van de NIS1-richtlijk moet duidelijk worden in de checklist. Dit is belangrijk omdat de organisaties die binnen het toepassingsbereik van de NIS1-richtlijn vallen, aan de verplichtingen van deze NIS-richtlijn moeten voldoen.
- De beveiligingseisen van de NIS1-richtlijn zijn een open norm. Aanbieders van essentiële diensten en digitale aanbieders dienen passende en evenredige maatregelen te treffen om de risico's voor de beveiliging van netwerk- en informatiesystemen te controleren. Hieruit vloeit de derde ontwerpeis: de beveiligingseisen van de NIS1-richtlijn moeten worden toegelicht in de checklist.

35 'Cybersecuritywet', *NJB* 2018/480.
36 Brouwer & Van Mil 2023, par. 2.3.1.
37 Art. 21 Richtlijn 2016/1148/EG.

- De bevoegde autoriteiten zijn verantwoordelijk voor de naleving van de NIS1-richtlijn. Hieruit vloeit de vierde ontwerpeis, namelijk: dat organisaties op de hoogte zijn van de verplichtingen van de richtlijn, zodat de richtlijn juist wordt toegepast.
- Incidenten met een aanzienlijk gevolg voor de continuïteit van de dienst moeten worden gemeld op grond van de NIS1-richtlijn. Hieruit vloeit de laatste ontwerpeis, namelijk dat de meldplicht in de checklist wordt beschreven, zodat organisaties hiervan op de hoogte zijn.

3.2 Ontwerpeisen verschillen en overeenkomsten NIS1-richtlijn en de Wet Beveiliging Netwerk- en Informatiesystemen

Om in kaart te brengen wat de verschillen en overeenkomsten zijn tussen de NIS1-richtlijn en de Wet Beveiliging Netwerk- en Informatiesystemen, hierna de WBNI, worden de richtlijn en de Nederlandse wettekst met elkaar vergeleken. In paragraaf 3.2.2 wordt er gekeken naar het toepassingsbereik, in paragraaf 3.2.3 naar de beveiligingseisen, in paragraaf 3.2.4 naar de bevoegde autoriteiten, in paragraaf 3.2.5 naar de meldplicht en in paragraaf 3.2.6 naar het toezicht, de handhaving en de sancties van de WBNI.

3.2.1 Inleiding Wet Beveiliging Netwerk- en Informatiesystemen

In de WBNI is de Europese NIS1-richtlijn omgezet naar het Nederlandse recht. Samen met de WBNI is ook het Besluit Beveiliging Netwerk- en Informatiesystemen, hierna het BBNI, in werking getreden. In het BBNI worden de vitale aanbieders aangewezen die binnen het toepassingsbereik van de verplichtingen van de WBNI vallen.[38] Daarnaast is de Wet Gegevensbescherming en Meldplicht Cybersecurity vanwege inhoudelijke samenhang en overlap in de WBNI opgenomen.[39] De Wet Gegevensbescherming en meldplicht is daardoor per 9 november 2018 komen te vervallen.[40]

3.2.2 Toepassingsbereik WBNI

In Nederland hanteert de WBNI een ruimer toepassingsbereik dan dat de NIS1-richtlijn voorschrijft. In de NIS1-richtlijn wordt er gesproken over aanbieders van essentiële diensten en in de WBNI over vitale aanbieders. Dit komt op hetzelfde neer, alleen worden er in de WBNI aanvullende vitale aanbieders aangewezen. In tabel 1 staat een overzicht van het toepassingsbereik van de NIS1- richtlijn en de WBNI.[41]

38 'Wet beveiliging netwerk- en informatiesystemen', nctv.nl.
39 'Wet beveiliging netwerk- en informatiesystemen', nctv.nl.
40 'Wettelijke taak', ncsc.nl.
41 Brouwer & Van Mil 2023, par. 2.1.2.

Tabel 1 | Overzicht toepassingsbereik NIS1-richtlijn en WBNI

NIS1-richtlijn	WBNI
Energie	Energie
Vervoer	Vervoer
Bankwezen	Bankwezen
Infrastructuur voor de financiële markt	Infrastructuur voor de financiële markt
Gezondheidszorg	Levering en distributie van drinkwater
Levering en distributie van drinkwater	Digitale infrastructuur
Digitale infrastructuur	Nucleair
	Financieel
	elektronische communicatienetwerken en- diensten/ICT
	Digitale overheid
	Keren en beheren (bijvoorbeeld sluizen en waterkeringen)

In de NIS1-richtlijn wordt aangegeven dat de richtlijn ook van toepassing is op de gezondheidszorg. In de WBNI ontbreekt deze sector doordat er voor de gezondheidszorg al een meldplicht voor incidenten bestaat. Daarnaast bestaat er voor de zorgsector al regels, toezicht en handhaving, zoals de meldplicht voor calamiteiten. Deze regels staan in de Wet kwaliteit, klachten en geschillen zorg, de meldplicht datalekken de beveiligingsvoorschriften en het toezicht daarop door de Inspectie Gezondheidszorg en Jeugd en de Autoriteit Persoonsgegevens.

De WBNI is ook van toepassing op aanbieders van digitale diensten. Aanbieders van digitale diensten vallen binnen het toepassingsbereik van de WBNI als het voldoet aan onderstaande voorwaarden:

1. de aanbieder van de digitale dienst moet een aanbieder van een online marktplaats, online zoekmachine of Cloudcomputerdienst zijn;[42]
2. het bedrijf moet 50 of meer medewerkers in dienst hebben of een jaaromzet of balanstotaal van meer dan 10 miljoen euro; en[43]
3. het bedrijf moet een Europese hoofvestiging in Nederland hebben of een vertegenwoordiging in Nederland hebben.[44]

42 Art. 4 sub 17, en sub 18, en sub 19 Richtlijn 2016/1148/EG.
43 *Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners* 2018, p. 5.
44 *Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners* 2018, p. 5.

3.2.3 Beveiligingseisen

De wettekst van de beveiligingsplicht in de WBNI is net zoals in NIS1-richtlijn een open norm.[45] Wel wordt er in de bijlage van de BBNI verwezen naar vijf maatregelen die zijn opgenomen die aanbieders van essentiële diensten ten minste moeten nemen. In bijlage 2 worden de maatregelen uitgebreider toegelicht, het gaat om de volgende vijf maatregelen:[46]

1. Risicogebaseerde aanpak: door het opstellen van een risicoanalyse waarin de risico's inzake de beveiliging worden beschreven en hoe deze risico's op een passend niveau kunnen worden verkleind.
2. Organisatie van netwerk- en informatiebeveiligingsbeheer: door het hebben en toepassen van een informatiebeveiligingsbeleid- en strategie.
3. Incidenten voorkomen: door het hebben van een gelaagde, technische beveiligingsstrategie die gebaseerd is op de risico's van de risicoanalyse.
4. Detectie en respons: door de beveiliging van netwerk- en informatiesystemen zo in te richten dat de aanbieder de incidenten kan analyseren, detecteren, vastleggen en monitoren om de gevolgen daarvan zo veel mogelijk te beperken.
5. Gevolgen van incidenten beperken: door het opstellen van een bedrijfscontinuïteitsbeleid en crisismanagementbeleid voor netwerk- en informatiesystemen.[47]

In het rapport 'Samenhangend Inspectiebeeld cybersecurity vitale processen 2023' staan een aantal voorbeelden van risico's die kunnen worden opgenomen in de risicoanalyse. Zo blijkt uit het rapport dat onrechtmatige inzage in dossiers of onnodige toegang tot systemen voor medewerkers leidde tot meerdere incidenten. Daarnaast blijkt uit het rapport dat vitale aanbieders over diverse incidenten en bevindingen onvoldoende overzicht hebben waartoe leveranciers toegang hebben. Het Nationaal Cyber Security Centrum, hierna NSCS, heeft een begeleiding gemaakt voor een 'logische toegangsbeveiliging'. Daarnaast adviseert het NSCS organisaties om risicomanagement toe te passen, gebaseerd op de weerbaarheid en dreigingen van de betreffende organisatie, om te bepalen of extra maatregelen nodig zijn.[48]

3.2.4 Bevoegde autoriteiten WBNI

De bevoegde autoriteiten zien op de handhaving van de WBNI. In Nederland is het centrale contactpunt van de bevoegde autoriteiten de Minister van Justitie en Veiligheid. In de WBNI wordt er onderscheid gemaakt tussen de functies van het CSIRT en de bevoegde autoriteiten. De bevoegde autoriteit is het Ministerie van Justitie en Veiligheid en voorziet in de functies: toezicht en sancties. Het CSIRT voorziet de functies: advies en bijstand. De Minister van Economische Zaken en Klimaat is aangewezen als het CSIRT voor digitale diensten. Voor vrijwillige incidentmeldingen is de Minister van Justitie en Veiligheid het zogenoemde 'loket'.[49]

45 Brouwer & Van Mil 2023, par. 2.2.2.
46 Bijlage van art. 3 sub a lid 1 BBNI.
47 Bijlage van art. 3 sub a lid 1 BBNI.
48 Samenhangend Inspectiebeeld cybersecurity vitale processen 2023, p. 14.
49 Artikel I van de wet van 17 oktober 2018 houdende regels ter implementatie van richtlijn (EU) 2016/1148 (Wet beveiliging netwerk- en informatiesystemen) (Stb. 2018, 387).

Daarnaast heeft de Nederlandse wetgever gekozen voor sectoraal toezicht. Sectoraal toezicht houdt in dat het toezicht per sector is geregeld. Omdat er sprake is van sectoraal toezicht zijn er diverse bevoegde autoriteiten aangewezen, bekijk hiervoor tabel 2.[50]

Tabel 2 | Sectoriaal toezicht

AED-sectoren	Bevoegde autoriteit	Toezichthoudende dienst
Energie	Minister van Economische Zaken en Klimaat	Rijkinspectie Digitale Infrastructuur (RDI)
Digitale infrastructuur	Minister van Economische zaken en Klimaat	Rijkinspectie Digitale Infrastructuur (RDI)
Bankwezen	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Infrastructuur voor de financiële markt	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Vervoer	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport
Levering en distributie van drinkwater	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport
Gezondheidszorg	Minister voor Medische zorg en Sport	Inspectie Gezondheidszorg en Jeugd

3.2.5 Meldplicht

De WBNI hanteert verschillende meldplichten voor vitale aanbieders en digitale dienstverleners. Een vitale aanbieder meldt een incident met aanzienlijke gevolgen voor de voortgang van de door hem verleende dienst en/of een schending op de beveiliging van netwerk- en informatiesystemen die aanzienlijke gevolgen kan hebben voor de voortgang van de door hem verleende dienst bij de NCSC.[51] Een digitale dienstverlener moet een incident melden bij de Rijksinspectie Digitale Infrastructuur en het CSIRT indien het gaat om een incident met aanzienlijke gevolgen voor de verlening van de door hem verleende dienst in de Europese Unie.[52] Om te bepalen of een incident aanzienlijke gevolgen heeft wordt er gekeken naar de volgende criteria.[53] Voor vitale aanbieders zijn punt 1, 2 en 3 van toepassing en voor digitale dienstverleners ook punt 4 en 5:

1. het aantal gebruikers dat door verstoring van de dienst wordt geraakt;
2. de duur van het incident;
3. de omvang van het geografisch gebied dat door het incident is geraakt;
4. de omvang van de verstoring van de werking van de dienst; en
5. de omvang van de gevolgen voor de economische en maatschappelijke activiteiten.

50 'Bevoegde Autoriteiten', nctv.nl.
51 Art. 13 lid 1 WBNI.
52 *Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners* 2018, p. 9.
53 Art. 10 lid 4 en art. 13 lid 2 WBNI.

Op grond van artikel 11 van de WBNI staan de volgende onderdelen in de melding:
1. de aard en omvang van het incident;
2. het vermoedelijke tijdstip van het incident;
3. de mogelijke gevolgen in en buiten Nederland van het incident;
4. een voorspelling van hersteltijd;
5. zo mogelijk, de door de aanbieder genomen of de te maatregelen om de gevolgen van het incident te beperken of herhaling te voorkomen; en
6. de contactgegevens van de functionaris die verantwoordelijk is voor het doen van de melding.[54]

Bij overschrijding van een specifieke drempelwaarde wordt een incident gemeld bij de toezichthouder.[55] De vitale aanbieder is verplicht alle informatie en gegevens te verstrekken aan de Minister van Justitie en Veiligheid. Zo kan de Minister de aanbieder onverwijld bij staan bij het nemen van maatregelen om de voortgang van zijn diensten te waarborgen en/of te herstellen, maar ook om de risico's in te schatten voor de netwerk- en informatiesystemen.[56] In 2022 zijn er geen incidenten gerapporteerd aan de toezichthouders die de drempelwaarde overschreden.[57] De digitale dienstverlener is verplicht alle informatie en gegevens te verstrekken aan het CSIRT. Zo kan het CSIRT de aanbieder onverwijld bij staan bij het nemen van maatregelen om de voortgang van zijn diensten te waarborgen en/of te herstellen, maar ook om de risico's in te schatten voor de netwerk- en informatiesystemen.[58]

3.2.6 Toezicht, handhaving en sancties

De bevoegde autoriteiten zijn belast met de bestuursrechtelijke handhaving van de WBNI.[59] De bevoegde autoriteiten kunnen gebruik maken van het handhavingsinstrumentenatrium ten aanzien van aanbieders van essentiële diensten en digitale dienstverleners. In de artikelen 5:11 tot en met 5:20 van de Algemene wet Bestuursrecht staan alle handhavingsbevoegdheden.[60] Allereerst hebben de bevoegde autoriteiten een auditbevoegdheid om door een onafhankelijke deskundige de organisatie te laten controleren. Dit door onderzoek te doen naar de naleving van de beveiligingsplicht. De resultaten van het onderzoek moeten binnen een redelijk gestelde termijn worden verstrekt aan de bevoegde autoriteit.[61] Mochten de beveiligingsplichten worden geschonden, dan kunnen de bevoegde autoriteiten nadere regels en aanwijzingen verplichten, zodat de voorgeschreven maatregelen alsnog kunnen worden genomen.[62] Ten tweede zijn de bevoegde autoriteiten bevoegd om ter handhaving een last onder bestuursdwang, last onder dwangsom of een bestuurlijke boete op te leggen.[63] De boete bedraagt 1 miljoen euro als het gaat om een overtreding van het niet verstrekken van gegevens aan de Minister of door geen medewerking te verlenen binnen de gestelde termijn. In het geval van een andere overtreding kan de boete oplopen tot 5 miljoen euro.[64]

3.2.7 Conclusie ontwerpeisen

Concluderend zijn dit de ontwerpeisen voor de checklist van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen die voortvloeien uit de verschillen en overeenkomsten tussen de NIS1-richtlijn en de WBNI:
- De NIS1-richtlijn is in Nederland geïmplementeerd in de WBNI. Hieruit vloeit de eerste ontwerpeis, namelijk: in Nederland zijn de verplichtingen van de WBNI van toepassing en daarom is de WBNI van belang voor de checklist.
- De WBNI is van toepassing op dezelfde zeven sectoren van de NIS1-richtlijn, behalve de gezondheidszorg. Daarnaast is de WBNI ook van toepassing op vijf andere sectoren. Hieruit vloeit de tweede ontwerpeis, namelijk: het toepassingsbereik van de WBNI in vergelijking met de NIS1-richtlijn.
- De beveiligingsplicht in de WBNI is een open norm. Wel schrijft de BBNI vijf basismaatregelen. Hieruit vloeit de derde ontwerpeis, namelijk: de vijf basismaatregelen van de BBNI. Organisaties binnen het toepassingsbereik van de WBNI moeten namelijk aan deze maatregelen voldoen.
- De bevoegde autoriteiten van de WBNI die zijn belast met de bestuursrechtelijke handhaving, zoals het opleggen van een last onder bestuursdwang of dwangsom. Hieruit vloeit de derde ontwerpeis, namelijk: organisaties op de hoogte stellen van de verplichtingen van de WBNI, zodat handhaving kan worden voorkomen.
- De meldplicht in de WBNI is anders dan de NIS1-richtlijn voorschrijft. In de WBNI wordt onderscheid gemaakt in de meldplicht voor 'vitale aanbieders' en 'digitale dienstverleners'. Hieruit vloeit de laatste ontwerpeis, namelijk: het verschil van de meldplicht moet duidelijk zijn voor vitale aanbieders en digitale dienstverleners in de checklist.

3.3 Ontwerpeisen wetsartikelen NIS2-richtlijn

De richtlijn 2022/2555 houdende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Europese Unie, hierna de NIS2-richtlijn genoemd, is de tweede richtlijn op het gebied van cybersecurity.[65] Sinds de werking van de NIS1-richtlijn is er progressie geboekt bij het vergroten van het niveau van digitale weerbaarheid van de Europese Unie. Toch is herziening van de NIS1-richtlijn noodzakelijk. De NIS1-richtlijn geeft een grote mate aan vrijheid aan de lidstaten en heeft daarom tot grote verschillen tussen de lidstaten gezorgd. Denk bijvoorbeeld aan het toepassingsbereik, verplichtingen rondom de meldplicht en het niveau van de cybersecurity. Daarnaast is ook het dreigingslandschap van netwerk- en informatiesystemen verandert. De NIS2- richtlijn moet de verschillen tussen de lidstaten wegwerken om zo een hoger gemeenschappelijk niveau van cybersecurity te bereiken.[66] De NIS2-richtlijn vervangt de NIS1-richtlijn die in Nederland is geïmplementeerd in de WBNI.[67]

54 Art. 11 WBNI.
55 *Samenhangend Inspectiebeeld cybersecurity vitale processen* 2023, p. 19.
56 Art. 12 lid 1 WBNI.
57 *Samenhangend Inspectiebeeld cybersecurity vitale processen* 2023, p. 19.
58 Art. 12 lid 1 WBNI.
59 Art. 4 lid 3 WBNI.
60 Art. 5:11-5:20 AWB.
61 Art. 26 lid 1 sub a WBNI.
62 Art. 27 WBNI.
63 Art. 28 WBNI.
64 Art. 29 WBNI.
65 Richtlijn (EU) 2022/2055 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (Nis 2-richtlijn) (*PbEU*, L 333)
66 Brouwer & Van Mil 2023, par. 1.
67 'Nieuwe cybersecurityrichtlijnen in werking getreden', *Computerrecht* 2023/72.

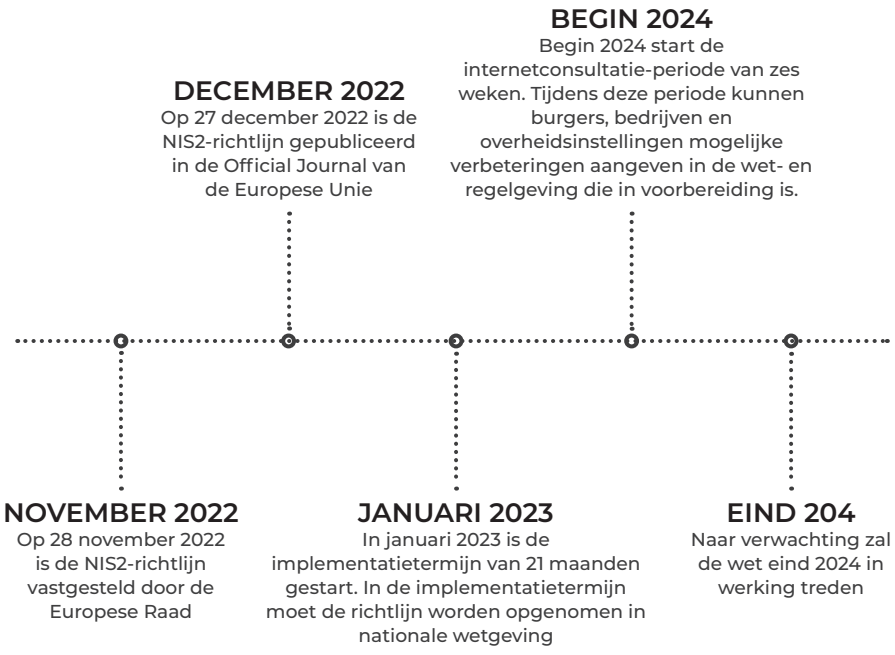
Om in kaart te brengen wat de toepasselijke wetsartikelen zijn van de NIS2-richtlijn worden de volgende onderwerpen besproken. In paragraaf 3.3.2 wordt het toepassingsbereik besproken, in paragraaf 3.3.3 de bevoegde autoriteiten, in paragraaf 3.3.4 de beveiligingseisen, in paragraaf 3.3.5 de meldplicht en in paragraaf 3.3.6 het toezicht, de handhaving en de sancties van de richtlijn.

3.3.1 Inleiding NIS2-richtlijn

De NIS2-richtlijn richt zicht op het hernieuwen van de digitale en economische weerbaarheid van de Europese lidstaten.[68] Het doel van de richtlijn is om de cybersecurity op een verbeterd niveau te brengen en te houden. Door de richtlijn hoopt de Europese Unie dat er meer informatie-uitwisseling en samenwerking rondom cybercrisisbeheer op de verschillende overheidsniveaus zal plaatsvinden.[69] Elke lidstaat van de Europese Unie moet op grond van artikel 7 van de NIS2-richtlijn beschikken over een nationale cyberbeveiligingsstrategie voor het bereiken en het in stand houden van een hoog niveau van cyberbeveiliging in de kritieke sector.[70] In bijlage 3 staat de nationale strategie.

3.3.1.1 De tijdlijn van de NIS2-richtlijn

In figuur 1 staat de tijdlijn van de implementatie van de NIS2-richtlijn:[71]



Figuur 1 | Tijdlijn NIS2-richtlijn

68 'NIS2-richtlijn', digitaleoverheid.nl.
69 Van Buuren 2023.
70 'Samenvatting van Richtlijn EU 2022/2555 - Cyberbeveiliging van netwerk- en informatiesystemen (2022)', eur-lex.europa.eu.
71 'Tijdlijn implementatie CER & NIS 2', nctv.nl.

3.3.2 Toepassingsbereik NIS2-richtlijn

Het toepassingsbereik van de NIS2-richtlijn wordt uitgebreid tot een groter deel van de economie. Dit om de sectoren en diensten die van belang zijn voor maatschappelijke en economische activiteiten, volledig in de hand te hebben.[72] De NIS2-richtlijn is van toepassing op achttien sectoren en maakt onderscheid tussen 'essentiële' en 'belangrijke' entiteiten. Daarnaast mag de Nederlandse overheid voor de NIS2-richtlijn ook kleine bedrijven met een hoog veiligheidsrisico aanwijzen.[73] Uit de webinar 'Wat je moet weten over NIS2' blijkt dat het verschil tussen essentiële en belangrijke entiteiten voornamelijk te maken heeft met het toezicht van de richtlijn en niet op de maatregelen die organisaties moeten treffen, bekijk hiervoor paragraaf 3.3.7.[74]

- **Essentiële entiteiten zijn grote organisaties die actief zijn in een sector uit tabel 2. Een essentiële** organisatie heeft minstens 250 werknemers of een jaaromzet van meer dan €50 miljoen en een balanstotaal van meer dan €43 miljoen.[75]
- **Belangrijke entiteiten zijn** middelgrote organisaties en grote organisaties. Een middelgrote organisatie heeft minstens 50 werknemers of een jaaromzet en balanstotaal van meer dan €10 miljoen.[76]

Tabel 3 | Sectoren NIS2-richtlijn

Essentiële entiteiten	Belangrijke entiteiten
Energie	Digitale aanbieders
Transport digitale infrastructuur	Post- en koeriersdiensten
Bankwezen	Afvalstoffenbeheer
Infrastructuur voor de financiële markt	Levensmiddelen
Transport	Chemische stoffen
Drinkwater	Onderzoek
Gezondheidszorg	Vervaardiging/manufacturing
Beheerders van ICT-diensten	
Afvalwater	
Overheidsdiensten	
Ruimtevaart	

De NIS2-richtlijn is van toepassing op de entiteiten in tabel 2 indien het gaat om:

- een organisatie dat gevestigd is in een lidstaat van de Europese Unie;
- de organisatie meer dan 50 werknemers in dienst heeft; en/of
- een jaaromzet en balanstotaal van meer dan 10 miljoen euro.

72 Overweging 6 van Richtlijn 2022/2555/EG.
73 Wondolleck & 't Hart 2023, par. 3.
74 'Wat je moet weten over NIS2 – NCTV', *Overheidsbreed Cyberprogramma*, weerbaredigitaleoverheid.nl, 21 november 2023 (webinar).
75 'Wat zijn de sectoren en criteria die bepalen of een organisatie onder de NIS2-richtlijn valt?', nctv.nl.
76 'Wat zijn de sectoren en criteria die bepalen of een organisatie onder de NIS2-richtlijn valt?', nctv.nl.

Daarnaast is de richtlijn op grond van artikel 2 lid 2 van de NIS2-richtlijn ook van toepassing op aanbieders van registers voor topleveldomeinnamen, elektronischecommunicatienetwerken, openbare elektronischecommunicatiediensten, verleners van domeinnaamregistratiediensten en aanbieders van vertrouwensdiensten. Ook is de NIS2-richtlijn van toepassing op een aantal uitzonderingen.[77] Deze uitzonderingen staan in bijlage 4.

3.3.3 Bevoegde autoriteiten

Elke lidstaat van de Europese Unie moet één of meer bevoegde autoriteiten aanwijzen of instellen. De bevoegde autoriteiten zijn verantwoordelijk voor de cyberbeveiliging en voor de toezichthoudende taken. Elke lidstaat van de Europese Unie gaat over tot het aanwijzen van een centraal contactpunt. Het centrale contactpunt heeft een verbindingsfunctie en zorgt voor grensoverschrijdende samenwerking van de autoriteiten van zijn eigen lidstaat en met belangrijke autoriteiten van andere lidstaten van de Europese Unie. Daarnaast moeten de bevoegde autoriteiten over de juiste middelen beschikken om de door hun toegewezen taken doeltreffend en efficiënt uit te voeren. De lidstaten van de Europese Unie moeten vaststellen welke capaciteiten, procedures en middelen in het geval van een crisis kunnen worden ingezet.[78]

3.3.4 Beveiligingseisen van de NIS2-richtlijn

In artikel 21 lid 2 sub a tot en met j van de NIS2-richtlijn staan de maatregelen voor het beheer van cyberbeveiligingsrisico's. Aangewezen entiteiten moeten de volledige cybersecurity van de organisatie toetsen aan de beveiligingsvereisten van de richtlijn. De NIS2-richtlijn bevat een uitgebreide en expliciete beveiligingsplicht die entiteiten verplicht om zelf een risicobeoordeling te doen en op basis daarvan maatregelen te nemen. Dit om diensten zoveel mogelijk te waarborgen en informatie te beschermen.[79] Daarnaast staat in de richtlijn dat bij het nemen van maatregelen entiteiten rekening moeten houden met de stand van techniek, Europese en internationale normen en met de uitvoeringskosten.[80] Het gaat om de volgende maatregelen:

- risicoanalyse en beveiliging van informatiesystemen;
- incidentenbehandeling;
- bedrijfscontinuïteit, denk aan back-upbeheer, noodvoorzieningenplannen en crisisbeheer;
- beveiliging van toeleveringsketen;
- beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen;
- beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
- basispraktijken op het gebied van cyberhygiëne, zoals: zero trust-beginselen, software updates, configuratie van apparaten, netwerksegementie, het vergroten van bewustzijn van cyberdreigingen en phishing en social engineering[81];
- opleiding op het gebied van cyberbeveiliging;
- beleid en procedures inzake het gebruik van cryptografie en encryptie;
- beveiligingsaspecten ten aanzien van personeel, toepassingsbeleid en beheer van activa; en
- gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-,video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit (indien van toepassing).

Daarnaast schenkt de NIS2-richtlijn ook aandacht aan de toeleveringsketen. Zo worden entiteiten in de NIS2-richtlijn aangemoedigd om cybersecuritymaatregelen overeen te laten komen in contracten met hun leveranciers en dienstverleners.[82] Het is belangrijk om cybersecuritymaatregelen te nemen bij toeleveringsketen, omdat beveiligingsproblemen zich vaak niet bij de entiteit zelf afspelen, maar bij de leverancier of dienstverlener.[83]

De bovenstaande maatregelen zijn de minimummaatregelen van de NIS2-richtlijn. De Europese Commissie kan de maatregelen door middel van uitvoeringshandelingen nader concretiseren en uitbreiden.[84] Daarnaast kunnen de lidstaten van de Europese Unie eisen dat de entiteiten bepaalde ICT-producten, ICT-processen en ICT-diensten gebruiken die door de entiteit zijn ontwikkeld of zijn gekocht bij een derde.[85]

De heer Palomo van Es van het Nationaal Coördinator Terrorismebestrijding en Veiligheid, hierna NCTV, is verantwoordelijk voor de cyberveiligheid in Nederland. De heer Palomo zegt tijdens de webinar 'wat je moet weten over NIS2' het volgende: "De implementatietermijn van de NIS2-richtlijn is in oktober 2024. Dat wil zeggen dat dan de Nederlandse wet- en regelgeving van kracht is en dat organisaties zich vanaf dat moment aan de verplichtingen moeten houden".[86] Daarom raadt hij organisaties aan om alvast een risicoanalyse te maken om te beoordelen welke belangen er van de organisatie moeten worden beschermd. Daarnaast raadt hij aan om processen in te richten op detectie, monitoring en response.[87]

3.3.5 Meldplicht NIS2-richtlijn

Er is sprake van een incident als er een gebeurtenis is die de beschikbaarheid van een dienst of van de verwerkte gegevens in gevaar brengt. In de NIS2-richtlijn moet er een melding worden gedaan als het gaat om een significant incident. Er is sprake van een 'significant incident' als de diensten van betrokken entiteiten operationeel worden verstoord of als er sprake is van financiële verliezen voor de betrokken entiteit. Daarnaast is er ook sprake van een significant incident als het incident andere natuurlijke personen of rechtspersonen treft of kan treffen door aanzienlijke materiële of door immateriële schade te veroorzaken.[88] In artikel 23 lid 4 van de NIS2-richtlijn staat het tijdspad waarbinnen de melding moet worden gedaan:

77 Art. 2 lid 2 sub b Richtlijn 2022/2555/EG.
78 Art. 8 Richtlijn 2022/2555/EG.
79 'NIS2-richtlijn', digitaleoverheid.nl.
80 Art. 21 lid 2 Richtlijn 2022/2555/EG.
81 Overweging 89 Richtlijn 2022/2555/EG.
82 Art. 21 lid 2 sub d Richtlijn 2022/2555/EG.
83 Overweging 85 Richtlijn 2022/2555/EG.
84 Art. 24 lid 2 Richtlijn 2022/2555/EG.
85 Art. 24 lid 1 Richtlijn 2022/2555/EG.
86 'Wat je moet weten over NIS2 – NCTV', *Overheidsbreed Cyberprogramma*, weerbaredigitaleoverheid.nl, 21 november 2023 (webinar).
87 'Wat je moet weten over NIS2 – NCTV', *Overheidsbreed Cyberprogramma*, weerbaredigitaleoverheid.nl, 21 november 2023 (webinar).
88 Art. 24 lid 2 sub a en sub b Richtlijn 2022/2555/EG.

- Onverwijld en binnen 24 uur na de kennisname van het incident moet een vroegtijdige waarschuwing worden gegeven. In de waarschuwing moet worden aangegeven of er sprake is van een onrechtmatige of kwaadwillige oorzaak en van mogelijke grensoverschrijdende gevolgen. Een snelle melding kan de gevolgen beperken.
- Onverwijld en binnen 74 uur na kennisname van het incident moet een incidentmelding worden gedaan. Daarin moet een initiële beoordeling van het incident worden opgenomen. In de boordeling moeten ook de ernst en de gevolgen van het incident worden meegenomen. Een grondige melding maakt het mogelijk om van voorgaande incidenten te leren.
- Binnen één maand na de melding van het incident moet een eindverslag worden ingediend. In het eindverslag moet een gedetailleerde omschrijving van het incident en de genomen cybersecuritymaatregelen worden genoemd.
- Indien het incident nog in beweging is na één maand, als het eindverslag moet worden ingediend, dan kan in plaats van een eindverslag een voortgangsverslag worden ingediend. Zodra het incident is afgehandeld, moet er alsnog binnen één maand het eindverslag worden ingediend.
- Indien er door het incident ook ontvangers van de verleende dienst worden geraakt, dan moeten de entiteiten de ontvangers ook onmiddellijk informeren over de maatregelen die zij kunnen nemen.[89]

3.3.6 Toezicht, handhaving en sancties NIS2-richtlijn

In de NIS2-richtlijn is er een verschil in toezicht voor essentiële en belangrijke entiteiten. Voor essentiële entiteiten is het toezicht proactief. Proactief toezicht vindt plaats op basis van vooraf vastgestelde prioriteiten, risico's of thema's. Voor belangrijke entiteiten is het toezicht reactief. Reactief toezicht vindt achteraf plaats, dit is vaak naar aanleiding van een melding en/of incident.[90]

Tijdens de webinar 'Wat je moet weten over NIS2' van de digitaleoverheid geeft de heer Heijligers van het Ministerie van Binnenlandse zaken en Koninkrijksrelaties aan dat de Rijksinspectie Digitale Infrastructuur (RDI) in Nederland het systeemgericht toezicht gaat houden. De RDI gaat controleren of het systeem overeenkomt met hoe het is ingericht bij de overheid. Waarschijnlijk krijgt de RDI de formele bevoegdheid om te gaan handhaven.[91]

In de NIS2-richtlijn is er een specifiek artikel over 'governance', namelijk: artikel 20 van de NIS2- richtlijn. Daarin staat dat de bestuursorganen de cybersecuritymaatregelen dienen goed te keuren, toe te zien op de uitvoering van de cybersecuritymaatregelen en entiteiten aansprakelijk kunnen stellen. Ook moeten de bestuurders zich, op grond van artikel 20, lid 2 van de NIS2-richtlijn, scholen door een cybersecurityopleiding te volgen. Bestuurders kunnen aansprakelijk worden gehouden bij non-compliance. Bestuurders kunnen in Nederland niet individueel als persoon aansprakelijk worden gesteld, dit geeft de heer Heijligers van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties aan tijdens de webinar 'wat je moet weten over de NIS2'.[92] Wel kunnen tegen de bestuurders handhavingsmaatregelen worden getroffen zoals een tijdelijk bestuursverbod.[93]

In de NIS2-richtlijn staat in artikel 32, lid 2 en artikel 33, lid 2 een opsomming van de onderzoeksbevoegdheden die de bevoegde autoriteiten ten minste moeten hebben. Ten eerste het uitvoeren van inspecties, daaronder valt ook het uitvoeren van een steekproef door een opgeleide professionals. Ten tweede het uitvoeren van beveiligingsaudits door een onafhankelijke instantie of een bevoegde autoriteit en ad-hocaudits. Tijdens een beveiligingsaudit wordt er gekeken naar het beveiligingsbeheer en de getroffen maatregelen, dit geeft inzicht over de mate van beveiliging en of de risico's in voldoende mate zijn afgedekt. Ad hoc houdt in dat er een onaangekondigd onderzoek plaatsvindt door een auditor. Tot slot het uitvoeren van beveiligingsscans en het opvragen van informatie, gegevens en andere documenten. Daarbij mogen de bevoegde autoriteiten organisaties verzoeken om toegang te geven tot gegevens, documenten, informatie en bewijs die nodig zijn voor de uitoefening van hun toezichthoudende taken.[94]

De lidstaten van de Europese Unie mogen sancties vaststellen die van toepassing zijn op inbreuken van de NIS2-richtlijn. De lidstaten van de Europese Unie moeten uiterlijk op 17 januari 2025 de Commissie kennis laten nemen van deze maatregelen en regels. Een voorbeeld van een sanctie is een boete. Op grond van artikel 34 van de NIS2-richtlijn kunnen er boetes worden opgelegd:

- Het boeteplafond voor belangrijke entiteiten is ten minste 7 miljoen euro of 1.4 procent van de totale wereldwijde omzet in het voorgaande financiële jaar.
- Het boeteplafond voor essentiële entiteiten is hoger, namelijk ten minste 10 miljoen euro of 2.0 procent van de totale wereldwijze omzet in het voorgaande financiële jaar.[95]

Indien er sprake is van een overtreding die ook een overtreding is op grond van de Algemene Verordening Gegevensbescherming, dan is er geen sprake van een dubbele boete. Wel kan er op grond van artikel 35 van de NIS2-richtlijn op een andere manier handhavend worden opgetreden.[96]

3.3.7 Conclusie ontwerpeisen NIS2-richtlijn

Concluderend zijn dit de ontwerpeisen voor de checklist van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen die voortvloeien uit de NIS2-richtlijn:

- Het doel van de NIS2-richtlijn is om de cybersecurity op een verbeterd niveau te brengen en te houden. Hieruit vloeit de eerste ontwerpeis, namelijk: het doel van de NIS2-richtlijn moet duidelijk worden omschreven in de checklist, zodat organisaties weten waarom de NIS2- richtlijn wordt geïntroduceerd.

89 Brouwer & Van Mil 2023, par. 3.3.
90 'Wat je moet weten over NIS2 – NCTV', *Overheidsbreed Cyberprogramma*, weerbaredigitaleoverheid.nl, 21 november 2023 (webinar).
91 'Wat je moet weten over NIS2 – NCTV', *Overheidsbreed Cyberprogramma*, weerbaredigitaleoverheid.nl, 21 november 2023 (webinar).
92 'Wat je moet weten over NIS2 – NCTV', *Overheidsbreed Cyberprogramma*, weerbaredigitaleoverheid.nl, 21 november 2023 (webinar).
93 Brouwer & Van Mil 2023, par. 4.2.
94 Art. 34 Richtlijn 2022/2055/EG.
95 Brouwer & Reijneveld 2023, par. 2.5.
96 Viergever & Van Til 2023, par. 7.

- Het toepassingsbereik van de NIS2-richtlijn. De NIS2-richtlijn is van toepassing op essentiële- en belangrijke entiteiten die behoren tot één van de achttien sectoren. Hieruit vloeit de tweede ontwerpeis, namelijk: het toepassingsbereik van de NIS2-richtlijk moet duidelijk worden in de checklist. Dit is belangrijk omdat de organisaties die binnen het toepassingsbereik van de NIS2-richtlijn vallen, aan de verplichtingen van deze richtlijn moeten voldoen.
- De NIS2-richtlijn bevat een uitgebreide en expliciete beveiligingsplicht. Organisaties moeten zelf een risicobeoordeling doen en op basis daarvan passende maatregelen nemen. Hieruit vloeit de derde ontwerpeis, namelijk: de beveiligingseisen van de NIS2-richtlijn moeten per eis worden toegelicht in de checklist, zodat het voor organisaties duidelijk is welke maatregelen de organisatie nog moet nemen. De implementatietermijn van de NIS2-richtlijn is in oktober 2024. De Nederlandse wet- en regelgeving is dan van kracht. Daarom wordt er in de webinar door het NCTV aangeraden om alvast voorbereidingen te treffen.
- Significante incidenten moeten op grond van de NIS2-richtlijn worden gemeld. Hieruit vloeit de vierde ontwerpeis, namelijk: dat de meldplicht in de uitwerking van de checklist wordt beschreven, zodat organisaties hiervan op de hoogte zijn.
- Voor essentiële entiteiten geldt er proactief toezicht en voor belangrijke entiteiten reactief. Daarnaast krijgen bevoegde autoriteiten de bevoegdheid om handhavend op te treden. Hieruit vloeit de laatste ontwerpeis, namelijk: de sancties in de uitwerking van de checklist beschrijven, zodat organisaties hiervan op de hoogte zijn en dit kunnen voorkomen.

3.4 Ontwerpeisen verschillen NIS1-richtlijn en NIS2-richtlijn

Om in kaart te brengen wat de verschillen zijn tussen de NIS1-richtlijn en de NIS2-richtlijn zijn beide richtlijnen met elkaar vergeleken. In paragraaf 3.4.1 wordt het verschil in toepassingsbereik besproken, in paragraaf 3.4.2 het verschil in beveiligingseisen, in paragraaf 3.4.3 het verschil in meldplicht en in paragraaf 3.4.4 het verschil in toezicht, handhaving en sancties. Ook wordt er in paragraaf 3.4.5. gekeken naar de verschillen van de ISO 27001/27002 normering en de NIS2-richtlijn.

3.4.1 Verschil in toepassingsbereik

De richtlijnen verschillen in toepassingsbereik. Waar de NIS1-richtlijn van toepassing is op zeven sectoren is de NIS2-richtlijn van toepassing op achttien sectoren waaronder ook middelgrote en kleine organisaties.[97] De heer Palomo van Es van het NCTV bevestigt dit en geeft aan dat de NIS1- richtlijn van toepassing is op ongeveer 350 organisaties en de NIS2-richtlijn op ongeveer 10.000 organisaties.[98] In tabel 3 worden de verschillende sectoren weergegeven.

97 'Welke sectoren en organisaties vallen onder de NIS2-richtlijn?', nscs.nl.

98 'Wat je moet weten over NIS2 – NCTV', *Overheidsbreed Cyberprogramma*, weerbaredigitaleoverheid.nl, 21 november 2023 (webinar).

Tabel 4 | Sectoren NIS1-richtlijn en NIS2-richtlijn

NIS1-richtlijn sectoren	NIS2-richtlijn sectoren
Energie	Energie*
Digitale infrastructuur	Transport Digitale infrastructuur*
Bankwezen	Bankwezen*
Infrastructuur voor de financiële markt	Infrastructuur voor de financiële markt*
Vervoer	Transport*
Levering en distributie van drinkwater	Drinkwater*
Gezondheidszorg	Gezondheidszorg*
	Beheerders van ICT-diensten*
	Afvalwater*
	Overheidsdiensten*
	Ruimtevaart*
	Digitale aanbieders**
	Post- en koeriersdiensten**
	Afvalstoffenbeheer**
	Levensmiddelen**
	Chemische stoffen**
	Onderzoek**
	Vervaardiging/manufacturing**

* = essentiële entiteiten

** = Belangrijke entiteiten

3.4.2 Verschil beveiligingseisen

Een ander verschil is dat de beveiligingseisen in de NIS2-richtlijn inhoudelijk zijn aangescherpt ten opzichte van de NIS1-richtlijn.[99] In de NIS1-richtlijn zijn de beveiligingseisen algemener geformuleerd. De NIS2-richtlijn is een verdieping van de NIS1-richtlijn, daardoor staan er in de NIS2-richtlijn meer specifieke en gedetailleerde maatregelen. Bijvoorbeeld de verplichting voor organisaties om cybersecurity-risico's in hun toeleveringsketen te adresseren. Daarnaast zijn er in de NIS2-richtlijn strengere eisen voor de strategische entiteiten, zoals overheden, defensie en de energiesector.

3.4.3 Verschil meldplicht

De meldingsdrempel in de NIS2-richtlijn is verlaagd. Dit houdt in dat er meer soorten incidenten verplicht moet worden gemeld. Als het gaat om de continuïteit van een dienst, dan gaat het om de NIS1-richtlijn. In de NIS2-richtlijn gaat het om een significant incident.[100] Een voorbeeld van een verschil van de meldingsdrempel is een ransomware-aanval. Op grond van de NIS1-richtlijn hoef je een ransomware-aanval niet te melden als de getroffen entiteit het losgeld

99 *Samenhangend Inspectiebeeld cybersecurity vitale processen* 2023, p. 19.

100 Wondolleck & 't Hart 2023, par. 4.

direct betaalt, omdat de duur van het incident beperkt is. Op grond van de NIS2-richtlijn moet, ondanks een directe betaling van losgeld door de getroffen entiteit, een ransomware-aanval wel worden gemeld. Dit komt omdat de getroffen entiteit een financieel verlies lijdt door de betaling van het losgeld en door de operationele verstoring die de ransomware-aanval teweeg heeft gebracht.[101]

3.4.4 Verschil toezicht, handhaving en sancties

De bepalingen met betrekking tot toezicht en handhaving zijn in de NIS2-richtlijn uitgebreider en strenger geformuleerd dan in de NIS1-richtlijn. Ten eerste moeten de bevoegde autoriteiten volgens de NIS1-richtlijn de nodige bevoegdheden en middelen hebben om de naleving van de beveiligingsplicht te kunnen beoordelen. In de NIS2-richtlijn staat dat de lidstaten van de Europese Unie ervoor moeten zorgen dat de bevoegde autoriteiten effectief toezicht houden op de naleving van de richtlijn en de noodzakelijke maatregelen daarvoor moeten nemen.[102]

Ten tweede introduceert de NIS2-richtlijn hogere sancties en boetes voor organisaties die zich niet aan de regels houden. Op dit moment is het boeteplafond 5 miljoen euro. Het boeteplafond voor belangrijke entiteiten kunnen ten minste 7 miljoen euro of 1.4 procent van de totale wereldwijde omzet in het voorgaande financiële jaar bedragen. Voor essentiële entiteiten kan dit zelfs ten minste 10 miljoen euro of 2 procent van de totale wereldwijde omzet in het voorgaande financiële jaar zijn. Daarnaast kunnen tegen bestuurders handhavingsmaatregelen worden getroffen en kunnen bestuurders aansprakelijk worden gesteld voor inbreuken op de beveiligingsverplichting. Een voorbeeld van een handhavingsmaatregel is een tijdelijk bestuursverbod.[103]

3.4.5 ISO 27001/27002 en de NIS2-richtlijn

De ISO 27001/27002 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. De ISO bevat eisen waar het managementsysteem voor informatiebeveiliging aan moet voldoen. De eisen worden onder andere toegepast op het implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging.[104] Voor een deel komen de eisen van de overeen met de NIS2-maatregelen. Een voorbeeld van eisen die overeenkomen is artikel 20 ‘Governance’ van de NIS2-richtlijn. Zo moet er op grond van de ISO de genomen maatregelen worden goedgekeurd en is er ook toezicht op de uitvoering van de maatregelen. Een voorbeeld van eisen die niet overeenkomen is het melden van incidenten met aanzienlijke gevolgen voor de verlening van diensten. In bijlage 5 staat de mapping van de Digitale Overheid met daarin de overeenkomsten en verschillen van ISO 27002 en de NIS2-richtlijn.[105]

101 N. Brouwer & J. van Mil 2023, par. 4.3.
102 N. Brouwer & J. van Mil 2023, par. 3.4.
103 N. Brouwer & J. van Mil 2023, par. 4.2.
104 ‘NEN-ISO/IEC 27001’, forumstandaardisatie.nl.
105 ‘Mapping NIS2-maatregelen’, digitaleoverheid.nl.

3.4.6 Conclusie ontwerpeisen verschillen NIS1-richtlijn en NIS2-richtlijn

Concluderend zijn dit de ontwerpeisen voor de checklist van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen die voortvloeien uit de verschillen en overeenkomsten van de NIS1-richtlijn en de NIS2-richtlijn:

- De NIS1-richtlijn is van toepassing op zeven sectoren en de NIS2-richtlijn is van toepassing op achttien sectoren. De sectoren van de NIS1-richtlijn zijn wederom ook van toepassing op de NIS2-richtlijn. Hieruit vloeit de eerste ontwerpeis, namelijk: het verschil in het toepassingsbereik beschrijven in de checklist.
- In de NIS1-richtlijn zijn de beveiligingseisen algemener geformuleerd. De NIS2-richtlijn is een verdieping van de NIS1-richtlijn, daardoor staan er in de NIS2-richtlijn meer specifieke en gedetailleerde maatregelen. Daarnaast komen ook een deel van de ISO maatregelen met de NIS2-richtlijn overeen. Hieruit vloeit de tweede ontwerpeis, namelijk: de beveiligingseisen van beide richtlijnen moeten worden omschreven in de checklist. Ook moeten de beveiligingseisen worden toegelicht in de uitwerking van de checklist.
- De meldingsdrempel is in de NIS2-richtlijn verlaagd. Dit houdt in dat er sneller sprake is van een incident dat moet worden gemeld. Hieruit vloeit de derde ontwerpeis, namelijk organisaties op de hoogte stellen van de meldplicht in de uitwerking van de checklist.
- Toezicht en handhaving is in de NIS2-richtlijn uitgebreider en strenger geformuleerd. Hieruit vloeit de laatste ontwerpeis, namelijk: het verschil in sancties in de uitwerking van de checklist beschrijven, zodat organisaties hiervan op de hoogte zijn en dit kunnen voorkomen.

4. Ontwerpeisen vanuit de praktijk

In dit hoofdstuk worden de praktijkdeelvragen beantwoord aan de hand van de uitkomsten van de afgenomen interviews, best practices en het testen van het beroepsproduct. Er wordt antwoord gegeven op de volgende deelvragen:

1. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen zijn af te leiden uit de kennis en ervaring van mkb-bedrijven met betrekking tot de uitvoering van de huidige NIS1-richtlijn?
2. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen zijn af te leiden uit de kennis en ervaring van mkb-bedrijven met betrekking tot de voorbereiding van de NIS2-richtlijn?
3. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen zijn af te leiden uit de kennis van de toezichthouders van de Wet Beveiliging Netwerk- en Informatiesystemen?
4. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen zijn af te leiden uit de NIS2 zelfevaluatie NL dat ontwikkeld is door de Rijksoverheid?
5. Welke ontwerpeisen voor de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen vloeien voort uit het testen van een concept checklist door medewerkers van de mkb-bedrijven?

Om erachter te komen wat de kennis en ervaringen zijn van mkb-bedrijven met betrekking tot de uitvoering van de NIS1-richtlijn en kennis en ervaring met betrekking tot de voorbereiding van de NIS2-richtlijn, zijn er interviewvragen gesteld aan drie verschillende organisaties. Organisatie A is een overheidsorganisatie in de drinkwatersector, gevestigd in Groningen en biedt drinkwater aan in de provincie Groningen en voor een deel in de provincie Drenthe. De organisatie hanteert op dit moment de Wet Beveiliging Netwerk- en Informatiesystemen (NIS1-richtlijn) en valt onder de (vitale) sector ‘levering en distributie van drinkwater’. De interviewvragenlijst die gesteld is aan organisatie A staat in bijlage 6.

Organisatie B is een organisatie in de telecomsector, gevestigd in Groningen en biedt telefonie aan in de Cloud voor bedrijven. De organisatie hanteert niet de Wet Beveiliging Netwerk- en

Informatiesystemen, aangezien zij als aanbieder van elektronische communicatiediensten (nog) niet vallen onder de norm van de BBNI van minimaal één miljoen eindgebruikers. De organisatie is wel ISO27001-gecertificeerd en geeft aan dat de organisatie aan vrijwel alle eisen van de Wet Beveiliging Netwerk en Informatiesystemen voldoet. De organisatie valt wel onder het toepassingsbereik van de NIS2-richtlijn wat betekent dat de organisatie aan de vereisten van de NIS2-richtlijn moet voldoen. De interviewvragenlijst die gesteld is aan organisatie B staat in bijlage 7.

Organisatie C is een softwarebedrijf op het gebied van debiteurenbeheer en is gevestigd in Groningen. De organisatie hanteert niet de Wet Beveiliging Netwerk- en Informatiesystemen aangezien ze niet valt onder het toepassingsbereik van deze wet. De organisatie is inmiddels acht jaar ISO27001-gecertificeerd. Op dit moment is het voor de organisatie nog onduidelijk of zij binnen het toepassingsbereik van de NIS2-richtlijn vallen, omdat de organisatie op dit moment ongeveer 40 medewerkers in dienst heeft. In het toepassingsbereik van de NIS2-richtlijn staat dat een organisatie minimaal 50 medewerkers in dienst moet hebben. Gezien de groei van de organisatie is de kans groot dat de organisatie in de toekomst wel binnen het toepassingsbereik van de NIS2-richtlijn gaat vallen. Daarnaast is de Nederlandse implementatie van de NIS2-richtlijn nog onbekend. Het kan zo zijn dat, net zoals in de Wet Beveiliging Netwerk- en Informatiesystemen, de Nederlandse implementatie van de NIS2-richtlijn ook van toepassing gaat zijn op meer sectoren dan de richtlijn op dit moment voorschrijft. De interviewvragenlijst die is gesteld aan organisatie C staat in bijlage 8.

Organisatie D is een overheidsorganisatie, gevestigd in Groningen en Amersfoort en is toezichthouder van de Wet Beveiliging Netwerk- en Informatiesystemen op het gebied van telecommunicatie en IT- netwerken in Nederland. Daarnaast is de toezichthoudende organisatie ook betrokken bij de totstandkoming en de implementatie van de NIS2-richtlijn. De interviewvragenlijst die is gesteld aan organisatie D staat in bijlage 9.

4.1 Ontwerpeisen kennis en ervaring van mkb-bedrijven met betrekking tot de uitvoering van de huidige NIS1-richtlijn

Om erachter te komen wat de kennis en ervaringen zijn van mkb-bedrijven met betrekking tot de uitvoering van de NIS1-richtlijn zijn er vragen over de NIS1-richtlijn en de Wet Beveiliging Netwerk- en Informatiesystemen gesteld aan organisatie A en organisatie B. De volgende punten zijn besproken met organisatie A en B. In paragraaf 4.1.1 wordt de cybersecurity binnen de organisaties en de getroffen maatregelen besproken en in paragraaf 4.1.2 de naleving van de WBNI en ISO. De toezicht, handhaving en meldplicht in paragraaf 4.1.3 is alleen met organisatie A besproken aangezien organisatie A binnen het toepassingsbereik van de WBNI valt en organisatie B niet.

4.1.1 Cybersecurity en maatregelen

Alle twee de organisaties vinden cybersecurity ontzettend belangrijk. Zo geeft organisatie A aan dat beveiliging de afgelopen jaren flink is veranderd. Zo werd er voorheen alleen aandacht besteed aan fysieke veiligheid, zoals het plaatsen van hekken om productielocaties. Nu heeft ICT een veel groter aandeel in de bedrijfsuitvoering en dat houdt in dat de cybersecurity op orde moet zijn aangezien je het als organisatie niet kan veroorloven dat daar iets mis gaat. Organisatie A valt onder een overkoepelende brancheorganisatie voor drinkwaterbedrijven, genaamd Vewin. Vewin is de partij die de belangen vertegenwoordigt bij de Inspectie Leefomgeving en Transport. Via Vewin is de organisatie op de hoogte dat de organisatie aan de wet- en regelgeving van de WBNI moet voldoen. Organisatie A heeft gezamenlijk met andere organisaties binnen de drinkwatersector gekeken wat de organisaties moeten gaan invoeren, om de NIS1-richtlijn voor de organisatie uitvoerbaar en toepasbaar te laten zijn. De organisaties binnen de sector hebben een werkgroep opgesteld met daarin de 43PA maatregelen. De 43PA maatregelen zijn maatregelen gebaseerd op de ISO27001 en de NIS1-richtlijn om netwerk- en informatiesystemen beter te beveiligen. Deze maatregelen heeft organisatie A voorgelegd aan de toezichthouder. De toezichthouder van de organisatie is de Inspectie Leefomgeving en Transport. De toezichthouder heeft de 43PA maatregelen goedgekeurd en is akkoord gegaan. Een voorbeeld van de 43PA maatregel is de toegangsbeveiliging. Organisatie A moet zowel fysiek als digitaal kunnen aantonen dat de toegangsbeveiliging goed geregeld is. Een ander voorbeeld is de toegangsrechten van het personeel. De toegangsrechten van een personeelslid moeten worden veranderd als het personeelslid op een andere afdeling gaat werken. Indien een personeelslid uit dienst gaat moeten alle toegangsrechten worden verwijderd.

Cybersecurity heeft een centrale rol bij organisatie B. Zowel voor het verwerken van klantgegevens, maar ook voor interne werkprocessen en bewustwording van medewerkers. Daarom heeft de organisatie verschillende maatregelen getroffen om beter beschermd te zijn tegen cyberaanvallen. Bijvoorbeeld door trainingen te geven over hoe om te gaan met phishing e-mails en het gebruiken van sterke wachtwoorden. Hierdoor wordt de bewustwording van cybersecurity onder medewerkers van de organisatie vergroot. Omdat organisatie B ISO27001-gecertificeerd is moet er kunnen worden aangetoond dat de informatiebeveiliging aan een systematische aanpak voldoet om gegevens te beschermen. Dit doet de organisatie door risico's te identificeren en op basis daarvan gepaste beveiligingsmaatregelen implementeren. Niet alleen de medewerkers van de organisatie moeten beveiligingsmaatregelen nemen, maar ook de klanten van de organisatie. Klanten en medewerkers moeten gebruik maken van twee-factor authenticatie. Waar dit voorheen een keuze was, heeft de organisatie dit nu verplicht gesteld om naast het wachtwoord ook een tweede identificatiemogelijkheid te gebruiken. Daarnaast zijn er extra maatregelen genomen om de toegang tot het pand te controleren. Iedereen die het pand binnenkomt moet zich verplicht inchecken en krijgt een eigen sleutel. Hierdoor weet de organisatie wie er wanneer binnenkomt en is er meer controle is over de toegang. Tot slot maakt organisatie B gebruik van diensten als Network based anti-DDoS Protection om de systemen te beschermen tegen aanvallen van buitenaf. De organisatie heeft maatregelen getroffen voor systeemherstel en continuïteit, zodat de systemen blijven werken tijdens eventuele storingen.

4.1.2 Naleving NIS1-richtlijn

Organisatie A geeft aan dat de naleving van de WBNI goed te doen is. Dit komt omdat de organisatie heeft aangegeven dat ze de beveiliging van netwerk- en informatiesystemen, ook voor de inwerkingtreding van de WBNI, al goed op orde hadden. Wel is het volgens de organisatie lastig om alle maatregelen continu te registreren. Het registreren van maatregelen

is namelijk een vereiste volgens de richtlijn. Organisatie A geeft aan dat het soms meer tijd kost om de maatregelen op papier te zetten, dan het daadwerkelijk beveiligen van de netwerk- en informatiesystemen. Dit gevoel heerst voor een groot deel bij de ICT-medewerkers die deze maartregelen en registratie uitvoeren. Een voorbeeld van het registeren van een maatregel is de toegangscontrole. Organisatie A geeft aan dat het beleid voor de toegangscontrole eenvoudig is geschreven, maar dat het daadwerkelijk kunnen aantonen lastiger is. Daarnaast moet de organisatie ook kunnen aantonen dat de maatregel geregeld gecontroleerd wordt en waar nodig aangepast. Dit kost veel tijd, geld en menskracht. Inmiddels is organisatie A bezig met het invoeren van een systeem waar alles in bijgehouden kan worden. Op dit moment gebeurt de registratie in verschillende losse systemen en daardoor verliest de organisatie soms het overzicht. Daarnaast is het volgens de organisatie belangrijk dat andere organisaties begrijpen welke maatregelen er getroffen moeten worden. De informatie in de wet- en regelgeving is immers beleidstaal en dat kan voor organisaties onduidelijk zijn. De organisatie adviseert andere organisaties om vanuit een risicobenadering naar de wet- en regelgeving te kijken. De organisatie geeft aan dat de WBNI moet worden gezien als een handreiking om de cyberrisico's van de organisatie in kaart te brengen om zo de organisatie beter te beschermen.

4.1.3 Toezicht, handhaving en meldplicht

De toezichthouder van organisatie A is de Inspectie Leefomgeving en Transport. Jaarlijks vindt er een interne audit plaats, dit houdt in dat er een onderzoek wordt gedaan binnen de organisatie naar het functioneren van bedrijfsprocessen en werkwijzen. De resultaten en bevindingen van de interne audit moeten met de toezichthouder worden gedeeld. Organisatie A deelt de plannen met de toezichthouder via een beveiligde verbinding. Op deze plannen wordt door de toezichthouder een oordeel gegeven en er worden aanvullende vragen gesteld. De toezichthouder komt daarnaast twee keer per jaar persoonlijk bij de organisatie langs, waaronder één keer per jaar in het kader van de WBNI. Van tevoren stuurt de toezichthouder de agenda met de punten die ze willen bespreken. Soms wil de toezichthouder van tevoren al documentatie inzien. Organisatie A geeft aan dit niet te verschaffen aangezien het vaak om vertrouwelijke informatie gaat. Tijdens de bijeenkomst zijn er deskundigen van de Inspectie Leefomgeving en Transport aanwezig die de organisatie door bepaalde processen heen loodsen met bepaalde vragen. De deskundigen gaan de diepte in en hebben volgens de organisatie een goed weerwoord. De organisatie ervaart de bijeenkomst dan ook als productief en leerzaam. Na de bijeenkomst wordt er een rapport gemaakt met de uitkomsten van de interne audit. Met de uitkomsten van het rapport proberen ze een sector breed rapport op te stellen om te kijken of er ergens een rode draad zit in de drinkwatersector. De sector heeft namelijk dezelfde normen voor beveiliging en zo kunnen de organisaties dezelfde beveiligingsnormen hanteren.

De toezichthouder van organisatie A heeft aangegeven niet meer te handhaven in het kader van de NIS1-richtlijn per 1 juni 2023. De reden hiervan is dat de toezichthouder het niet redelijk vindt om te handhaven aangezien er een grote kans bestaat dat de implementatie van de NIS2-richtlijn niet tijdig klaar gaat zijn. Organisaties weten dan nog niet exact wat er van hen verwacht gaat worden aangezien de Nederlandse implementatie kan afwijken van de wettekst uit de NIS2-richtlijn.

Daarnaast heeft de toezichthouder medegedeeld dat het persoonlijk bezoek per 2024 niet meer plaatsvindt. De NIS2-richtlijn is voor meer organisaties van toepassing en daarom is het niet haalbaar om alle organisaties persoonlijk te bezoeken. De toezichthouders blijven wel via een audit monitoren. Naast de jaarlijkse interne audit, vindt er ook één keer per vier jaar een externe audit plaats. Een externe audit houdt in dat er door een onafhankelijke externe partij getoetst wordt of de processen binnen het bedrijf effectief en doeltreffend zijn. De resultaten van de externe audit worden meegenomen in de beveiligingsplannen van de organisatie. Er wordt gekeken naar de volgende punten: hoe staat de organisatie ervoor, wat gaat niet goed en wat zijn de verbeterplannen. Dit is een verplichting vanuit de Inspectie Leefomgeving en Transport.

Organisatie A is goed op de hoogte van de meldplicht. Ondanks het feit dat de organisatie nog nooit te maken heeft gehad met een incident dat moet worden gemeld op grond van de meldplicht. Organisatie A geeft daarom ook aan geen voorbeelden te kunnen geven van een ervaring met de meldplicht. Wel staat de meldplicht in het calamiteitsplan van de organisatie opgenomen. Organisatie A geeft aan dat incidenten met aanzienlijke gevolgen voor de netwerk- en informatiesystemen van de organisatie moeten worden gemeld. In het calamiteitsplan staat onder andere het preventief waarschuwen en handelen. Zo heeft de organisatie een deels ingevulde rapportage die waar nodig nog moet worden aangevuld. In de rapportage staat onder andere de aard en omvang van het incident, de mogelijke gevolgen van het incident en het tijdstip wanneer het incident heeft plaatsgevonden. De rapportage moet zo snel mogelijk naar een speciaal e-mailadres worden gestuurd en er moet worden gebeld met een specifiek telefoonnummer. Mocht er een incident plaatsvinden waar meerdere organisaties in betrokken zijn, dan wordt de melding van het incident gedaan door de veiligheidsregio. Bij de veiligheidsregio heeft de organisatie een centraal aanspreekpunt. Organisatie A geeft de informatie aan het centrale contactpunt van de veiligheidsregio en de veiligheidsregio coördineert de informatie verder aan de nodige partijen. Voor de komst van de NIS1-richtlijn had de organisatie dit ook al vrijwillig geregeld met de veiligheidsregio. Dit komt omdat de organisatie de veiligheidsregio in bepaalde gevallen nodig is voor informatievoorziening en afhankelijk van het incident voor hulp en bijstand.

4.1.4 Conclusie ontwerpeisen

Concluderend zijn dit de ontwerpeisen voor de checklist van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen die voortvloeien uit de kennis en ervaring van mkb-bedrijven met betrekking tot de uitvoering van de NIS1-richtlijn:

- Cybersecurity wordt in de praktijk ontzettend belangrijk geacht. Het is daarom belangrijk om ervoor te zorgen dat netwerk- en informatiesystemen goed worden beveiligd. Hieruit vloeit de eerste ontwerpeis, namelijk: het belang van cybersecurity benadrukken in de checklist.
- Alle maatregelen die een organisatie neemt moeten aantoonbaar worden gemaakt. Dit kost veel tijd en mankracht. Hieruit vloeit de tweede ontwerpeis, namelijk: Alle maatregelen van de NIS-richtlijnen moeten worden geregistreerd en het is belangrijk om dit zo efficiënt mogelijk in te richten. Het is belangrijk om organisaties hier aan de hand van de checklist op te adviseren.

- De toezichthouder controleert de naleving van de NIS1-richtlijn door jaarlijks een audit uit te voeren en op basis daarvan een rapport op te stellen. Hieruit vloeit de derde ontwerpeis, namelijk dat het belangrijk is om aan de maatregelen te voldoen aangezien hier jaarlijks toezicht op is.
- Voor incidenten met aanzienlijke gevolgen voor netwerk- en informatiesystemen is er een meldplicht. Hieruit vloeit de laatste ontwerpeis, namelijk: het is belangrijk om een incidentenmeldingen vast te leggen in een calamiteitenplan, zodat een incident direct kan worden gemeld.

4.2 Ontwerpeisen kennis en ervaring van mkb-bedrijven met betrekking tot de voorbereiding van de NIS2-richtlijn

Om erachter te komen wat de kennis en ervaringen zijn van mkb-bedrijven met betrekking tot de voorbereiding van de NIS2-richtlijn zijn er vragen gesteld aan organisatie A, B en C. In paragraaf 4.1.2 wordt besproken de cybersecurity en maatregelen van organisatie C. In paragraaf 4.2.2 wordt de kennis en voorbereiding van de NIS2-richtlijn besproken, in paragraaf 4.2.3 de impact van de richtlijn en in paragraaf 2.3.4 wat de organisaties over de richtlijn willen weten.

4.2.1 Cybersecurity en maatregelen

Organisatie C vindt cybersecurity ontzettend belangrijk aangezien e organisatie in het bezit is van veel klantgegevens, bedrijfsgevoelige gegevens en privacygevoelige gegevens. Daarom hebben ze besloten om zich ISO 27001 te laten certificeren. De organisatie is inmiddels acht jaar in het bezit van een ISO27001-certificaat. Organisatie C geeft tijdens het interview aan: “In het begin was het een uitdaging om de eisen van ISO 27001 na te leven, met name op procedurele vlak. Toen wij acht jaar geleden begonnen met ISO was dit een behoorlijke uitdaging. In het begin waren er veel feedbackpunten en het verwerken van de feedback kost veel tijd. Naarmate de jaren is de organisatie steeds beter beschermd en worden de aanpassingen minder. Vooral voor startende bedrijven met een klein team kan het hanteren van extra beveiligingseisen lastig zijn”. Daarnaast heeft de organisatie de processen zo ingericht dat ze kunnen controleren hoe goed de cybersecurity op technisch gebied is. Daarnaast zijn er periodieke controles, zoals: awareness trainingen bij medewerkers en trainingen voor developers die werken met privacygevoelige gegevens. Recentelijk heeft de organisatie een training gevolgd genaamd ‘red team, blue team exercise’. Tijdens de training wordt het development team in tweeën opgesplitst. Team red moet team blue aanvallen, een soort hack, team blue moet zich vervolgens verdedigen. Dit is een goede test om te kijken of team red team de mogelijkheden kan vinden om te hacken en voor team blue of deze hack eenvoudig kan worden gerepareerd.

4.2.2 Kennis en voorbereiding van de NIS2-richtlijn

Organisatie A en B zijn op de hoogte dat de NIS2-richtlijn eraan komt, maar zijn enigszins nog aan het afwachten op de Nederlandse implementatie van de NIS2-richtlijn. Organisatie A wil kijken of ze aan de NIS2-richtlijn een eigen invulling kunnen geven voor de drinkwatersector, net zoals ze bij de NIS1- richtlijn hebben gedaan. De afdeling ICT van de organisatie is op dit moment aan het onderzoeken welke aanpassingen de organisatie moet treffen voor de NIS2-richtlijn. Na de jaarlijkse audit van begin 2024, wil de organisatie uitgebreider onderzoek gaan doen naar de NIS2-richtlijn en daadwerkelijk de nodige maatregelen treffen.

Organisatie B is op de hoogte van de komst van de NIS2-richtlijn. Het is voor de organisatie nog onduidelijk wat de exacte implicaties gaan zijn. De organisatie anticipeert op de mogelijke wijzigingen, maar willen voor de voorbereiding de implementatie van de nationale wetgeving afwachten aangezien het nog afwachten is wat er concreet per lidstaat van een organisaties verwacht gaat worden. Zodra dit bekend is gaat de organisatie met de League cirkel in gesprek om in kaart te brengen wat de implicaties zijn en waar de organisatie rekening mee moet houden. Vervolgens worden deze punten meegenomen naar het securityteam om de technische implicaties uit te voeren. Aangezien de organisatie ISO27001-gecerfiticeerd is, verwachten ze dat ze voor een groot deel al NIS2-richtlijn zullen voldoen. Specifieke vragen die de organisatie heeft over de NIS2- richtlijn gaan over hoe de meldplicht en de beveiligingseisen. Vooral in vergelijking met de NIS1- richtlijn en ISO 27001 aangezien ze op dit moment de ISO 27001 normering hanteren. Of de vereisten van de NIS2-richtlijn eenvoudig na te leven zijn vinden ze op dit moment lastig te beoordelen.

Organisatie C geeft aan niet op de hoogte te zijn van de huidige NIS1-richtlijn en de WBNI. Sterker nog, de organisatie heeft nog nooit van de NIS1-richtlijng gehoord. Naar aanleiding van het interview heeft de organisatie de NIS2-richtlijn besproken met de externe adviseur. Hierdoor weten ze dat, ze gezien de ISO 27001, voor een groot deel aan de vereisten van de NIS2-richtlijn zullen voldoen. Aan de hand van de zelfevaluatie van de Rijksoverheid weet de organisatie dat ze op dit moment nog niet onder het toepassingsbereik van de NIS2-richtlijn vallen. In de zelfevaluatie kunnen organisaties er namelijk achter komen of ze binnen het toepassingsbereik van de NIS2-richtlijn vallen, bekijk hiervoor hoofdstuk 4.4. Gezien de groei van de organisatie is de kans groot dat de organisatie hier over een aantal jaar wel onder valt. Dat houdt in dat de organisatie dan wel aan de vereisten van de NIS2-richtlijn moet voldoen. Daarom vindt de organisatie het belangrijk om wel op de hoogte te zijn van de NIS2-richtlijn en zich waar nodig voor te bereiden.

4.2.3 Impact NIS2-richtlijn

Organisatie A verwacht dat de impact van de NIS2-richtlijn op de organisatie meevalt aangezien de organisatie op dit moment de WBNI hanteert. Wel geeft de organisatie aan dat er binnen de afdeling ICT wel enige zorg is over de richtlijn. Zo moet er in de WBNI voor procesautomatisering alle wijzigingen worden bijgehouden. De organisatie geeft aan dat dit veel tijd kost en dat ze dit na drie jaar nu redelijk op orde hebben. De zorg van de ICT afdeling is dan ook of het haalbaar is om alle wijzigingen in de systemen ook voor de NIS2-richtlijn bij te houden. Organisatie A verwacht namelijk dat dit gaat om ‘nog’ meer wijzigingen. Door de hoeveelheid wijzigingen zijn ze bang dit niet voor elkaar te krijgen. Ook geeft de organisatie aan dat het registreren van wijzigingen onoverzichtelijk kan worden aangezien sommige wijzigingen ook door andere personeelsleden worden uitgevoerd. Daarnaast vinden sommige wijzigen automatisch plaats door systemen en dit maakt het aantonen lastig.

Organisatie B verwacht dat de impact van de NIS2-richtlijn niet groot gaat zijn aangezien de organisatie ISO27001-geretificeert is. Wel verwacht de organisatie dat de impact voor mkb-bedrijven groot gaat zijn, de organisatie zegt hierover het volgende: “het gaat hier om bedrijven die voorheen niet onder de NIS1-richtlijn vielen, maar wel aan de vereisten van de NIS2-richtlijn moeten voldoen. Het naleven van de richtlijn kost veel tijd en mankracht. Met name voor organisaties die geen ISO- certificaat hebben en/of weinig juridische kennis”.

Organisatie C vindt het lastig om in te schatten wat de impact van de NIS2-richtlijn gaat zijn aangezien de organisatie ISO27001-gecertificeert is. De organisatie is met name benieuwd naar de impact op klanten en leveranciers aangezien de organisatie op dit moment ook niet met bepaalde leveranciers samen werkt die niet ISO27001-gecertificeerd zijn. Dit komt omdat klanten zich hier ook steeds meer bewust van zijn. Als de organisatie bijvoorbeeld gegevens van klanten moet verstrekken aan leveranciers, dan moeten de leveranciers wel voldoen aan de eisen van de organisatie. Zo vraagt de organisatie zich het volgende af: “indien wij de NIS2-richtlijn moeten hanteren en gegevens van klanten aan leveranciers verstrekken, moeten de leveranciers dan ook aan de eisen van de NIS2- richtlijn voldoen?”

4.2.4 Wat willen organisaties over de NIS2-richtlijn weten?

Organisatie A wil weten welke punten van de NIS2-richtlijn van toepassing gaat zijn op de drinkwatersector en dan met name punten die op dit moment niet in de WBNI gelden. Daarnaast geeft de organisatie aan benieuwd te zijn naar de rol van de bestuurders aangezien de organisatie op de hoogte is dat bestuurders aansprakelijk gesteld kunnen worden.

Organisatie B is benieuwd naar de implementatie van de nationale wetgeving en welke extra eisen er gaan komen met betrekking tot de NIS1-richtlijn. Daarnaast is de organisatie benieuwd hoe de meldplicht van de NIS2-richtlijn eruit komt te zien. Op grond van de Algemene Verordening Gegevensbescherming is er ook een meldplicht als het gaat om datalekken. De organisatie vraagt zich af of er dan een dubbele melding van een datalek moet worden gegeven, namelijk van de Algemene Verordening Gegevensbescherming en de NIS2-richtlijn.

Voor organisatie C is de huidige NIS1-richtlijn onbekend. Zoals het nu lijkt hoeft de organisatie niet aan de NIS2-richtlijn te voldoen, maar wellicht in de toekomst wel. De organisatie wil daarom graag weten wat de impact voor de organisatie zelf gaat zijn, maar ook de impact op de klanten en leveranciers. Daarnaast zouden ze een externe adviseur of jurist moeten inschakelen om de wettekst juist te vertalen. Op dit moment heeft organisatie geen jurist in dienst, omdat er voor een jurist geen fulltime werk is. De organisatie verwacht dat de meeste mkb-bedrijven geen jurist in dienst hebben en dat het lastig kan zijn om wetteksten juist te interpreteren. Ook verwachten ze een voordeel te hebben met de ISO 27001 in tegenstelling tot andere organisaties die niet in het bezit zijn van een ISO certificaat. Ondanks dat de organisatie op dit moment niet onder het toepassingsbereik van de NIS2-richtlijn valt, wilt de organisatie wel alvast actie ondernemen. Organisatie C gaat de ISO 27001 en NIS2-richtlijn met elkaar vergelijken om te bepalen welke eisen van de NIS2-richtlijn nog ontbreken. Aan de hand van de vergelijking worden de ontbrekende eisen toegevoegd binnen de organisatie om zo aan de vereisten van de NIS2-richtlijn te voldoen.

4.2.5 Advies voor organisaties

Organisatie A wil organisaties adviseren om tijd te nemen om de richtlijn juist te interpreteren aangezien het belangrijk is om het belang van de richtlijn in te zien. De organisatie wil als tip meegeven om hier de tijd voor te nemen. De organisatie geeft aan dat organisaties de vereisten van de NIS2-richtlijn als handvatten kunnen gebruiken om ervoor te zorgen dat de cybersecurity binnen de organisatie op orde is. Dit is ook een goede uitstraling voor klanten en leveranciers. De organisatie adviseert organisaties daarom tijdig te beginnen. Dit kan aan de hand van een risicoanalyse. Zodra in kaart is gebracht waar de risico’s zitten van de organisatie, kan op basis daarvan de juiste beveiligingsmaatregelen worden getroffen. De organisatie wil als tip meegeven om alle beveiligingsmaatregelen goed te regristreten, zodat de organisatie de getroffen maatregelen kan aantonen.

Organisatie B wil organisaties adviseren om dit vanuit een intrinsieke motivatie te doen. De NIS2- richtlijn biedt hiervoor mogelijkheden. De organisatie geeft het volgende aan: “iedere klant wil dat er met zijn of haar informatie zorgvuldig wordt omgegaan en dat een organisatie hier een grote bijdrage aan levert. Daarnaast kan het nooit kwaad om netwerk- en informatiesystemen beter te beveiligen. Organisaties B wil dan ook andere organisaties adviseren om meerdere keren per jaar kritisch te kijken naar de risico’s van de organisatie. Reflecteer op wat gaat er goed en waar moet de organisatie nog aandacht aan besteden. Maak voor de aandachtspunten vervolgens een plan om deze punten te verbeteren. Probeer deze cirkel vervolgens draaiende te houden. Zo zorg je ervoor dat een organisatie continu bewust is met de cybersecurity binnen de organisatie”.

Organisatie C wil organisaties adviseren om zo vroeg mogelijk actie te ondernemen. Als de organisatie er vroegtijdig bij is, kan de organisatie klein beginnen en langzamerhand extra punten toevoegen aan cybersecurity. Onder andere bewustzijn bij het personeel kost veel tijd en veranderingen kunnen voor weerstand zorgen. De organisatie wil andere organisaties dan ook adviseren om kleine stappen te nemen om zo langzamerhand de cybersecurity te verbeteren. Daarnaast geeft de organisatie aan dat er ook leuke manieren zijn om het personeel bewust te maken van cybersecurity. De organisatie heeft bijvoorbeeld een bot geïnstalleerd in de communicatiesystemen en vertelt hierover het volgende: “zodra een personeelslid zijn laptop niet lockt kunnen de andere personeelsleden hier een melding van maken, ook wel ‘snipen’ genoemd. Op het leaderboard kan het gehele team zien wie de meeste ‘snipes’ heeft. De personeelsleden willen zo min mogelijk ‘snipes’ hebben en daarom let het personeel er daarom goed op om de laptop te locken. De eerste paar maanden werden personeelsleden geregeld ‘gesniped’, maar dit komt nu veel minder vaak voor. Dit is een voorbeeld om bewustzijn onder het personeel op een leuke manier over te brengen. Dit zorgt ook voor minder weerstand, aangezien de bewustwording op een leuke manier in de organisatie wordt toegepast”.

4.2.6 Conclusie ontwerpeisen

Concluderend zijn dit de ontwerpeisen voor de checklist van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen die voortvloeien uit de kennis en ervaring van mkb-bedrijven met betrekking tot de voorbereiding op de NIS2-richtlijn:

- Cybersecurity wordt in de praktijk ontzettend belangrijk geacht. Het is daarom belangrijk om ervoor te zorgen dat netwerk- en informatiesystemen goed worden beveiligd. Hieruit vloeit de eerste ontwerpeis, namelijk: het belang van cybersecurity benadrukken in de checklist.
- De impact van de NIS2-richtlijn kan in de praktijk groot zijn. Al helemaal voor organisaties die op dit moment nog niet onder de WBNI valt of niet in het bezit zijn van een ISO27001-certificaat. Hieruit vloeit de tweede ontwerpeis, namelijk: organisaties informeren om tijdig te beginnen met de voorbereiding op de NIS2-richtlijn.

- De wetteksten uit de NIS2-richtlijn kunnen voor organisaties zonder juridische kennis lastig te interpreteren zijn. Hieruit vloeit de derde ontwerpeis, namelijk: de teksten in de checklist in begrijpelijke taal schrijven en verwijzen naar een extra uitleg pagina.
- Organisaties zijn enigszins afwachtend van de Nederlandse Implementatie van de NIS2-richtlijn. De toezichthouder van organisatie A heeft aangegeven dat de verwachtingen zijn dat de Nederlandse implementatietermijn niet gehaald gaat worden. Hieruit vloeit de laatste ontwerpeis, namelijk: dat het belangrijk is om aan de verplichtingen van de NIS2-richtlijn te voldoen en niet wachten tot de Nederlandse implementatie bekend is.

4.3 Ontwerpeisen kennis van de toezichthouders van de Wet Beveiliging Netwerk- en Informatiesystemen

Om erachter te komen wat de kennis en ervaringen zijn van toezichthouders met betrekking tot de WBNI zijn er vragen gesteld aan organisatie D. In paragraaf 4.3.1 staat hoe het huidige toezicht eruit ziet in de WBNI en wat de verwachtingen voor het toezicht gaan zijn met betrekking tot de NIS2- richtlijn. Daarnaast wordt in 4.3.2 de implementatie van de NIS2-richtlijn besproken en in 4.3.3 het advies van organisatie D voor andere organisaties.

4.3.1 Toezicht WBNI en verwachtingen toezicht NIS2-richtlijn

Organisatie D legt uit dat er twee soorten toezicht zijn in de WBNI, namelijk: ex-ante toezicht en ex- post toezicht. Ex-ante toezicht, ook wel proactief toezicht, geldt voor aanbieders van essentiële diensten waar toezicht op moet worden gehouden. De organisatie geeft aan dat dit een beperkte groep is en dat het gaat om tientallen partijen. Ex-ante toezicht is intensief en de toezichthoudende organisatie gaat dan ook geregeld bij deze organisaties langs voor zowel gesprekken over de ontwikkeling, maar ook voor reguliere inspecties. Een reguliere inspectie kan gaan over de volle breedte van cybersecurity binnen een organisatie, maar ook over een specifiek thema. De organisatie noemt als voorbeeld een inspectie over business continuity management. Tijdens de inspectie wordt bepaald hoe een organisatie omgaat met een grote cybersecuritycrisis. Daarnaast is er ex-post toezicht, ook wel reactief toezicht. Ex-post toezicht geldt voor digitale dienstverleners. Ex- post toezicht houdt in dat organisatie D een inspectie gaat uitvoeren als ze signalen krijgen dat er bij een partij iets niet goed geregeld is. De signalen krijgt de organisatie doordat een klant een melding heeft gedaan, er iets over in de media staat of dat er door eigen onderzoek achter wordt gekomen.

Organisatie D is als toezichthouder met name bezig met de naleving van de zorgplicht. Dit wordt gedaan aan de hand van de vijf domeinen in de BBNI, maar ook door te kijken naar algemene normen zoals bijvoorbeeld de ISO 27001. Aan de hand daarvan wordt gekeken hoe organisaties aan deze normen invulling hebben gegeven. De context van de organisatie wordt daarin meegenomen. Er zijn namelijk grote organisaties die wereldwijd actief zijn en een groot budget hebben en kleine organisaties waarin de bedrijfsvoering anders is en waarin cybersecurity ook anders wordt georganiseerd. Hier wordt dan ook rekening mee gehouden.

De toezichthouder geeft aan dat er naar aanleiding van een toezichtgesprek een rapport wordt opgesteld met daarin de bevindingen van het gesprek. In het rapport staat met name wat er beter kan. Het is afhankelijk van de aard van de bevindingen hoe daar opvolging aan wordt gegeven. Als de bevinding bijvoorbeeld ernstig zijn, dan zitten de toezichthouders daar bovenop zodat het snel wordt opgelost. Als het gaat om minder erge bevindingen, dan krijgen organisaties meer tijd om dat onderdeel op orde te brengen. De verantwoordelijkheid ligt in ieder geval altijd bij de partijen zelf. De partij moet zelf met een plan komen van hoe de organisatie de risico's wil gaan beheersen. Organisatie D toetst vervolgens of dat plan navolgbaar is. In extreme situaties kan organisatie D een bindende aanwijzing geven of een last onder dwangsom opleggen, maar dit is volgens de organisatie voor de sectoren van de WBNI nog niet aan de orde geweest.

Op dit moment vindt er toezicht plaats bij essentiële organisaties die binnen het toepassingsbereik van de WBNI vallen. Voor de NIS2-richtlijn moeten toezichthouders gaan prioriteren hoe er toezicht wordt gehouden en op welke manier. De toezichthouders gaan kijken wat de publieke belangen zijn die beschermd moeten worden en waar de grootste maatschappelijke risico's op zitten. Op basis daarvan gaan ze prioriteren binnen de groep van partijen die onder toezicht staan. Daar gaan de toezichthouders intern kaders voor opstellen. De methode om de organisaties fysiek te bezoeken kan niet meer in de toekomst. Er moet volgens de toezichthoudende organisatie in ieder geval een goed afwegingskader komen die elke keer weer kan worden toegepast. Daarnaast speelt bestuurdersverantwoordelijkheid in de NIS2-richtlijn ook een grote rol. Hierin is het belangrijk dat een organisatie het organisatorisch goed op orde heeft. De toezichthouder geeft aan dat dit eigenlijk een basisvoorwaarde is voor een goede werking in de praktijk. Hier gaat de toezichthoudende organisatie dan ook zeker aandacht aan besteden. Hoe het toezicht er precies uit komt te zien kan de toezichthoudende organisatie nog niet delen aangezien de organisatie dit nu aan het opzetten is.
Ook kan de toezichthoudende organisatie nog niet delen of er voor de NIS2-richtlijn meer toezichthouders en toezichthoudende partijen bij gaan komen.

4.3.2 Implementatie NIS2-richtlijn in de Wet Beveiliging Netwerk- en Informatiesystemen

Over de implementatie van de NIS2-richtlijn in de WBNI kan de toezichthoudende organisatie geen informatie geven. Zo ook niet of de implementatietermijn wel of niet gehaald gaat worden. Wel zegt de organisatie hier het volgende over: "Als de NIS2-richtlijn niet tijdig geïmplementeerd is kun je daar als toezichthouder niet op gaan handhaven. Een richtlijn heeft namelijk geen directe werking en is niet direct verbindend. Als het een verordening was geweest, dan was dit anders. Daarnaast is de NIS2-richtlijn feitelijk al in werking getreden alleen is er een deadline voor de omzetting van de richtlijn in nationale wetgeving voor de lidstaten. Per oktober 2024 moet de NIS2-richtlijn geïmplementeerd zijn in nationale wetgeving. Als dat in oktober 2024 nog niet gebeurd is, dan hoeven partijen zich niet direct aan de verplichtingen van de NIS2-richtlijn te houden. Dit moet pas als het in de Nederlandse wet staat dat organisaties daaraan moeten voldoen. Er zijn eventuele kleine uitzonderingen voor uitvoeringshandelingen die wel rechtstreekse werking kunnen hebben, afhankelijk van hoe ze zijn opgesteld. Maar nieuwe partijen met betrekking tot de NIS2-richtlijn, hebben geen verplichtingen als de Nederlandse wet niet tijdig is geïmplementeerd". Wel raadt de toezichthoudende organisatie aan om alvast aan de slag te gaan met de verplichtingen van de NIS2- richtlijn aangezien het veel tijd kan kosten om de cybersecurity binnen een organisatie op orde te hebben. Daarnaast kan de Nederlandse implementatie ook wel tijdig zijn afgerond en dan moet er al wel aan de verplichtingen van de NIS2-richtlijn worden voldaan.

4.3.3 Advies voor organisaties

Organisatie D wil organisaties adviseren om alvast te budgetteren voor cybersecurity de komende boekjaren aangezien cybersecurity nooit af is en het veel tijd kost om cybersecurity op orde te krijgen en te houden. Daarnaast is het ook belangrijk om te bepalen wie welke rol en verantwoordelijkheid heeft voor de cybersecurity binnen een organisatie. Er moet worden gekeken hoe er vanuit het management goed zicht is op de staat van cybersecurity van de organisatie en de financiering daarvan. Verder is het volgens de organisatie goed om te kijken wat een organisatie op dit moment al doet aan cybersecurity en hoe je dat kunt uitbreiden en toepassen voor de WBNI.

Voor organisaties met weinig juridische kennis, adviseert organisatie D aan om een adviseurs in te schakelen. Een adviseur kan bijvoorbeeld een overzicht maken met wat er juridisch gezien van een organisatie wordt verwacht. Daarnaast kan een adviseur ook bijvoorbeeld helpen met het maken van een risicoanalyse. De toezichthouder geeft namelijk aan dat cybersecurity uiteindelijk risicomanagement is en dat 100% veiligheid niet bestaat. Een organisatie moet kijken wat het verschil binnen de organisatie gaat maken gezien de belangen die er moeten worden beschermd en de bedreigingen die daar tegenover staan.

4.3.4 Conclusie ontwerpeisen

Concluderend zijn dit de ontwerpeisen voor de checklist van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen die voortvloeien uit de kennis van de toezichthouders van de Wet Beveiliging Netwerk- en Informatiesystemen:

- Op dit moment vindt er ex-ante (proactief) toezichtplaats voor essentiële entiteiten. Voor digitale dienstverleners is het toezicht ex-post (reactief). Voor de NIS2-richtlijn is het toezicht voor essentiële entiteiten ex-ante en voor belangrijke entiteiten ex-post. Hieruit vloeit de eerste ontwerpeis, namelijk: het verschil in toezicht voor essentiële en belangrijke entiteiten uitleggen in de uitwerking van de beveiligingseisen.
- Voor de NIS2-richtlijn moeten toezichthouders gaan prioriteren hoe er toezicht gehouden gaat worden. Er moet een goed afwegingskader komen. Daarnaast speelt bestuurdersverantwoordelijkheid een belangrijke rol in de NIS2-richtlijn. Hieruit vloeit de tweede ontwerpeis, namelijk: voor de NIS2-richtlijn komt het toezicht er anders uit te zien, waarin bestuurdersverantwoordelijkheid ook een grote rol gaat spelen. Het verschil in toezicht, in hoeverre bekend, moet worden meegenomen in de uitwerking van de checklist.
- Als de NIS2-richtlijn niet tijdig geïmplementeerd is in de WBNI, dan hoeven nieuwe organisaties zich niet direct aan de verplichtingen van de richtlijn te houden. Als de richtlijn wel tijdig is geïmplementeerd, dan moet er wel aan de verplichtingen worden voldaan. Hieruit vloeit de derde ontwerpeis, namelijk: dat het belangrijk is om alvast aan de verplichtingen van de NIS2-richtlijn te voldoen ongeacht of de implementatie termijn in Nederland gehaald gaat worden. Het treffen van cybersecurity maatregelen kost namelijk veel tijd.
- De toezichthoudende organisatie adviseert om alvast te budgetteren voor cybersecurity, te bepalen wie welke verantwoordelijkheid heeft voor cybersecurity en om te kijken hoe huidige maatregelen kunnen worden toegepast voor de WBNI. Hieruit vloeit de laatste ontwerpeis, namelijk: dat organisaties budgetteren voor cybersecurity maatregelen.

4.4 Ontwerpeisen uit de NIS2 zelfevaluatie dat ontwikkeld is door de Rijksoverheid

Voor dit onderzoek is er gekeken naar de zelf-evaluatie van de Rijksoverheid voor organisaties om erachter te komen of de NIS2-richtlijn op de organisatie van toepassing is. Door de zelfevaluatie kan een organisatie bepalen of de NIS2-richtlijn van toepassing is op de organisatie, of de organisatie onder een ‘essentiële’ of ‘belangrijke’ entiteit valt en of de organisatie valt onder het Nederlandse toezicht. In paragraaf 4.4.1 worden de stappen besproken en in paragraaf 4.4.2 de uitkomst. De vragen die worden gesteld kunnen per sector verschillen.

4.4.1 De stappen van de zelfevaluatie

Om erachter te komen of de NIS2-richtlijn van toepassing is op de organisatie worden er een aantal vragen gesteld in de zelf-evaluatie. De vragen moeten beantwoord worden en aan de hand daarvan komt het uiteindelijke resultaat.[106]

1. De allereerste stap van de zelfevaluatie is om toestemming te geven op het disclaimerakkoord. Het disclaimerakkoord wil zeggen dat, ondanks de zorgvuldigheid van de test, aan de uitkomst van de zelfevaluatie geen rechten kunnen worden ontleend.
2. De tweede stap is om alle sectoren te selecteren die van toepassing zijn op de organisatie. Zodra er een sector wordt aangevinkt staat er onderaan de pagina direct welk ministerie verantwoordelijk is. Daarnaast is er ook de mogelijkheid om op een blauw vinkje met vraagteken te drukken voor meer informatie over de sector.
3. Vervolgens moeten er in sommige gevallen sub sectoren worden geselecteerd. Bij sommige sectoren zijn er geen sub sectoren van toepassing, zoals de sectoren: afvalstoffenbeheer, onderzoek en productie, verwerking en distributie van chemische stoffen. In dat geval wordt de stap van sub sectoren overgeslagen.
4. Vervolgens komt de vraag of de organisatie in Nederland gevestigd is.

Indien de organisatie in Nederland gevestigd is wordt er gekeken naar de volgende drie punten:

1. Hoeveel medewerkers er werkzaam zijn. Er is hier de keuze uit drie mogelijkheden: 1-49, 50- 249 of 250 of meer.
2. De hoogte van de jaaromzet van het laatst gesloten boekjaar. Er is hier de keuze uit drie mogelijkheden: minder dan 10 miljoen euro, 10-50 miljoen euro of meer dan 50 miljoen euro.
3. En de balans van het laatst afgesloten boekjaar. Er is hier de keuze uit drie mogelijkheden: minder dan 10 miljoen euro, 10-43 miljoen euro of meer dan 43 miljoen euro.

106 ‘NIS2 Zelfevaluatie NL’, regelhulpenvoorbedrijven.nl.

4.4.2 Uitkomst zelfevaluatie

Afhankelijk van de uitkomst van de bovenstaande drie vragen en/of als de organisatie niet in Nederland gevestigd is, wordt er bepaalt of er in Nederland een bekende uitsluiting en uitzondering zijn voor de organisatie. Daarnaast wordt er gekeken of er sectorspecifieke cyberwetgeving van toepassing is op de organisatie en of er sprake is van een kritiek belang.

- Een voorbeeld voor een uitzondering is dat de organisatie in Nederland de enige aanbieder is van een dienst die essentieel is voor de instandhouding van kritieke maatschappelijke of economische activiteiten.
- Een voorbeeld voor een uitsluiting kan zijn de nationale veiligheid of als er sectorspecifieke cyberwetgeving is.
- Een voorbeeld voor kritiek belang is als de organisatie al eerder is aangewezen als essentiële entiteit.

Ook als er geen bekende uitsluitingen en geen sectorspecifieke cyberwetgeving van toepassing is op de organisatie, kan het zo zijn dat de organisatie wel aan de vereisten van de NIS2-richtlijn moet voldoen als belangrijke entiteit. Dit kan verschillen per sector en per organisatie.

Op basis van bovenstaande punten wordt er gekeken of de NIS2-richtlijn van toepassing is op de organisatie. De uitkomst van de zelfevaluatie staat onderaan de pagina onder het kopje ‘resultaat’ en kan worden gedownload. In het gedownloade document staat nogmaals of de organisatie wel of niet aan de NIS2-richtlijn moet voldoen. Daarnaast staan er ook een aantal verplichtingen van de NIS2- richtlijn in, zoals: de zorgplicht, de meldplicht en toezicht.

Het voordeel van de zelf-evaluatie van de Rijksoverheid is dat organisaties de mogelijkheid hebben om per vraag door te klikken. De zelf-evaluatie past zich aan op de antwoorden die worden gegeven door de organisatie.

4.4.3 Conclusie ontwerpeisen

Concluderend zijn dit de ontwerpeisen voor de checklist van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen die voortvloeien uit de zelf-evaluatie van de Rijksoverheid:

- In de zelf-evalutatie van de Rijksoverheid kunnen organisaties erachter komen of de organisatie binnen het toepassingsbereik van de NIS2-richtlijn valt. Hieruit vloeit de volgende ontwerpeis, namelijk: alle stappen die een organisatie bij langs moet gaan om te controleren of een organisatie binnen het toepassingsbereik van de NIS2-richtlijn valt. Dit zijn de volgende stappen: het kiezen van de sectoren die van toepassing zijn op de organisatie, de vraag of de organisatie in Nederland is gevestigd, de vraag hoeveel werknemers de organisatie in dienst heeft, de vraag of het jaaromzet en balanstotaal meer dan 10 miljoen is en of er eventuele uitzonderingen van toepassing zijn. Deze stappen worden toegepast in de checklist.

4.5 Ontwerpeisen van het testen van een concept checklist door medewerkers van de mkb-bedrijven

In hoofdstuk vier worden de verschillende versies van de checklist besproken. In paragraaf 4.5.1 wordt de eerste versie van de checklist besproken, deze is aangepast naar aanleiding van feedback van de opdrachtgever. Vervolgens wordt in paragraaf 4.5.2 de tweede versie van de checklist besproken, deze is aangepast naar aanleiding van feedback van drie organisaties van het praktijkonderzoek. In paragraaf 4.5.3 de definitieve versie van de checklist besproken. Tot slot wordt er in paragraaf 4.5.4 de uitkomst gedeeld van het testen van de checklist door de drie organisaties van het praktijkonderzoek.

4.5.1 Eerste versie checklist

Ten eerste is er een eerste versie van de checklist gemaakt. In bijlage 11 staat de eerste versie van de checklist. De eerste versie is op 17 november 2023 met de opdrachtgever besproken doormiddel van een gesprek. De opdrachtgever heeft de checklist voor het gesprek bekeken en beoordeelt en tijdens het gesprek is dit kenbaar gemaakt. De feedback is vervolgens verwerkt in de checklist. De volgende punten zijn naar aanleiding van het gesprek aangepast:

- Het logo is aangepast. In de eerste versie is het logo van het Lectoraat Juridische Aspecten van de Hanzehogeschool gebruikt, maar dit moet het logo van Cybersecurity Noord Nederland zijn.
- Het kopje ‘basismaatregelen’ is verwijderd. Het gaat in dit kopje om de basismaatregelen van cyberhygiëne. Deze basismaatregelen worden wel besproken in de uitwerking van de beveiligingseisen. Via de QR-code rechts onderaan de hoek wordt naar de uitwerking verwezen. Er is gekozen om dit niet op de checklist zelf uit te leggen aangezien dit te veel tekst bevat. Tevens zouden andere kopjes dan ook uitgebreider moeten worden geformuleerd aangezien daar ook meer uitleg over wordt gegeven in de uitwerking. De uitwerking via de QR-code biedt daarvoor de oplossing.
- Er is voor een andere titel gekozen. De titel was eerst ‘checklist NIS2-richtlijn’ en dit is aangepast naar ‘checklist NIS2-richtlijn voor uw organisatie’. Hiervoor is gekozen zodat er in de andere kopjes niet continu naar ‘uw organisatie’ hoeft worden te verwezen.
- De kopjes tekst op de pagina van de beveiligingseisen zijn aangepast. Zo zijn de kopjes in dezelfde schrijfstijl geschreven. Voorheen waren sommige kopjes algemeen en andere kopjes werden persoonlijk gemaakt door ‘uw organisatie’ erin te verwerken. De schrijfstijl is nu overal gelijk.

4.5.2 Tweede versie checklist

Naar aanleiding van bovenstaande feedback, is er een tweede versie van de checklist gemaakt. In bijlage 12 staat de tweede versie van de checklist. Voor de tweede versie is bij de drie organisaties van het praktijkonderzoek om feedback gevraagd. Dit feedback moment heeft direct na het interview plaatsgevonden op 21 november, 22 november en 12 december 2023. Bij twee van de drie organisaties heeft dit gesprek plaatsgevonden op locatie van de organisatie en bij de andere organisatie was dit online via Teams. Tijdens het gesprek zijn er de volgende feedback vragen gesteld:

- is de checklist overzichtelijk en gebruiksvriendelijk?
- is alle informatie in de checklist voor jullie relevant?
- wat zijn de positieve punten van de checklist?

- welke punten kunnen er beter worden beschreven in de checklist?
- wat ontbreekt er nog in de checklist?
- wou u de checklist kunnen toepassen binnen uw organisatie?

Alle drie de organisaties waren enthousiast over de checklist en zouden de checklist willen toepassen binnen de organisatie. Wel hadden de organisaties ook feedback op de checklist. Onderstaand de feedback punten die zijn verwerkt in de tweede versie van de checklist.

- Op de voorkant is er duidelijker omschreven wanneer je onder het toepassingsbereik van de NIS2-richtlijn valt. Op dit moment was het voor organisatie C namelijk nog onduidelijk. Dit zit hem met name in de drie kopjes: hoeveelheid werknemers, jaaromzet en balanstotaal. Voorheen stonden deze punten in één kopje verwerkt, dat is aangepast naar drie verschillende kopjes.
- Daarnaast geeft organisatie A aan dat het voor organisaties niet relevant is om te weten of de organisatie een belangrijke- of essentiële entiteit is aangezien beide entiteiten dezelfde beveiligingsmaatregelen moeten toepassen. Voorheen stonden boven de sectoren of het een belangrijke- of essentiële entiteit is, dit is nu verwijderd. Of een organisatie essentieel is wordt nu aan de hand van één ster (*) duidelijk.
- Er staat in een kopje van de beveiligingseisen ‘tegen’ cryptografie en encryptie, dit moet zijn ‘voor’ cryptografie en encryptie.
- Ook geeft de organisatie aan sommige teksten in kopjes onduidelijk te vinden. Tijdens de feedback waren de QR-codes nog niet werkzaam. De QR-codes geven meer duidelijkheid aan deze kopjes. Alle beveiligingseisen worden namelijk toegelicht in een uitwerking. Door de QR-code te scannen komt de organisatie op de juiste pagina met de uitwerkingen terecht.

4.5.3 Definitieve versie checklist

Naar aanleiding van bovenstaande punten, is er een derde versie van de checklist gemaakt. Er zijn nog een aantal wijzigingen doorgevoerd naar aanleiding van het gesprek met de opdrachtgever van donderdag 21 december 2023. Tijdens dit gesprek zijn de verwerkte feedbackpunten besproken en is over sommige onderdelen advies gevraagd. Uiteindelijk zijn deze punten verwerkt in de checklist en is er een definitieve versie tot stand gekomen. In bijlage 13 staat de definitieve versie van de checklist. Dit zijn de laatste aanpassingen van de checklist:

- Op de voorkant van de checklist stond ‘in een ander lidstaat’, dit moet zijn ‘in een andere lidstaat’. Het woord ‘ander’ is aangepast naar ‘andere’.
- Op de voorkant van de checklist staat er onder de sectoren één ster (*) of twee sterren (**). Eén ster houdt in dat de sector kan worden aangemerkt als essentiële entiteit. Twee sterren staat voor zowel essentiële entiteiten en dat de sector ook al binnen het toepassingsbereik van de NIS1-richtlijn viel. In de definitieve versie is ervoor gekozen om niet de één ster toe te passen voor essentiële entiteiten. Er zit namelijk geen onderscheid in de beveiligingseisen voor essentiële entiteiten en andere entiteiten. Het is wel handig om te weten of de sector ook al binnen het toepassingsbereik van de NIS1-richtlijn viel. Daarom worden deze sectoren met één ster aangeduid.
- Stap drie op de voorkant van de checklist is net iets duidelijker geformuleerd. Stap drie staat in twee kopjes beschreven. Via een pijl wordt er van het eerste kopje naar het tweede kopje verwezen. Daarnaast staat er in het tweede kopje en/of. Dit kan soms onduidelijk zijn, omdat er niet altijd naar het tweede kopje hoeft worden gekeken. Indien een organisatie namelijk meer dan 50 werknemers in dienst heeft, kan direct naar de volgende stap worden gegaan en hoeft er niet naar het vak ernaast (het tweede vak) worden gekeken. Het pijltje is daarom vervangen met een boogje met daarboven het woord ‘of’. Daarnaast worden de woorden en/of in het begin van het tweede vak weggehaald.
- Tot slot zijn de QR-codes onderaan de pagina aangepast. Voorheen werkte de QR-codes nog niet, maar zijn ze puur als voorbeeld aan de checklist toegevoegd. Inmiddels werken de QR- codes en wordt er verwezen naar de juiste pagina’s.

4.5.4 Testen checklist

De drie organisaties van het praktijkonderzoek die ook feedback hebben gegeven op de checklist, zijn individueel gevraagd om de checklist te testen. Gedurende de test is het van belang dat de organisaties de checklist eenvoudig kunnen raadplegen. Daarnaast moeten de organisaties een inzicht krijgen of de organisatie onder het toepassingsbereik van de NIS2-richtlijn valt. Ook kunnen de organisaties aan de hand van de checklist eenvoudig afvinken welke vereisten ze op dit moment al naleven en/of aan welke vereisten de organisatie nog moet voldoen. De checklist is één dag voor het ‘testgesprek’ gemaild naar de drie organisaties, zodat de organisaties de checklist alvast konden testen. In de mail voor het testgesprek stonden ook alvast een aantal vragen, zodat hier gedurende het testen rekening mee kon worden gehouden. Het testgesprek van 4 januari heeft plaatsgevonden via teams en het testgesprek van 9 januari 2024 heeft plaatsgevonden op locatie van de organisatie. De volgende vragen uit de mail zijn tijdens het testgesprek besproken:

- Werkt de checklist gebruiksvriendelijk en is de checklist overzichtelijk?
- Kunt u naar aanleiding van de checklist erachter komen of uw organisatie binnen het toepassingsbereik van de NIS2-richtlijn valt?
- Is het duidelijk welke beveiligingseisen de NIS2-richtlijn voorschrijft?
- Zou u de checklist willen toepassen binnen uw organisatie?
- Zijn er nog verbeterpunten?

Uit het testen van de checklist bleek het volgende:

- Alle drie de organisaties kunnen de checklist raadplegen. De checklist is overzichtelijk en gebruiksvriendelijk.
- De organisaties geven uit dat de nieuwe versie helderder is dan de vorige versie waar feedback op is gegeven.
- Het is eenvoudig om aan de hand van de checklist erachter te komen of een organisatie binnen het toepassingsbereik van de NIS2-richtlijn valt. Soms is het lastig om in te schatten in welke sector een organisatie precies valt, maar met behulp van de QR-code wordt hier meer duidelijkheid aan gegeven. De QR-code verwijst naar de zelf-evaluatie van de Rijksoverheid en daarin wordt per sector uitgelegd wat voor organisaties daar onder vallen.
- De beveiligingseisen staan duidelijk geformuleerd. Sommige beveiligingseisen zijn in eerste instantie voor de organisaties nog wat onduidelijk, maar met behulp van de QR-code kunnen de organisaties hier meer informatie over vinden. Ook zijn de beveiligingseisen herkenbaar voor de organisaties die op dit moment al ISO27001-gecertificeerd zijn. De beveiligingseisen zijn volgende de organisaties dan ook goed uitgelegd.

- Er is een laatste aanpassing gedaan om het woord phising aan te passen naar phishing in de uitwerking van de beveiligingseisen.
- Kortom: de organisaties zijn enthousiast over de checklist en willen de checklist toepassen binnen de organisatie.

4.5.5 Conclusie ontwerpeisen

Concluderend zijn dit de ontwerpeisen voor de checklist van het lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen die voortvloeien uit de feedback en het testen van de checklist:

- De checklist is meerdere malen van feedback voorzien door de opdrachtgever en de organisaties van het praktijkonderzoek en is uiteindelijk ook getest door de organisaties van het praktijkonderzoek. Naar aanleiding van de feedback is de checklist waar nodig aangepast.
- De vormgeving en schrijfstijl in de checklist is aangepast. Zo is het logo van Cybersecurity Noord-Nederland toegevoegd, is de schrijfstijl overal gelijk gemaakt, is de titel aangepast en zijn sommige kopjes weg gelaten en in de uitwerking toegevoegd.
- Het toepassingsbereik van de NIS2-richtlijn is duidelijker omschreven. Er is een apart kopje gemaakt met de vraag hoeveel werknemers een organisatie in dienst heeft en een apart kopje met de vraag over het jaaromzet en balanstotaal.
- De checklist wordt als overzichtelijk en gebruiksvriendelijk ervaren. De organisaties willen de checklist dan ook graag toepassen binnen de organisatie.

5. Analyse en conclusie

In hoofdstuk 5 zijn de ontwerpeisen van het theorie- en praktijkonderzoek met elkaar vergeleken. In paragraaf 5.1 wordt het handelingsprobleem besproken, in paragraaf 5.2 wordt de centrale onderzoeksvraag herhaald en in paragraaf 5.3 worden de ontwerpeisen vanuit verschillende onderzoeksobjecten uit de praktijk met elkaar vergeleken. Op basis van bovenstaande punten wordt in paragraaf 5.5 een conclusie getrokken en wordt antwoord gegeven op de centrale onderzoeksvraag.

5.1 Het handelingsprobleem

De NIS1-richtlijn is de eerste richtlijn om cybersecurity in de Europese Unie te verbeteren en om eenheid te brengen in het Europese beleid voor netwerk- en informatiebeveiliging. Gezien de ontwikkelingen van de afgelopen jaren wordt de maatschappij en economie steeds meer onder druk gezet. Daarom is sinds 2020 vanuit de Europese Unie aan de NIS2-richtlijn gewerkt. De NIS2-richtlijn wordt momenteel omgezet in nationale wetgeving. De NIS2-richtlijn moet in oktober 2024 zijn geïmplementeerd. In Nederland wordt de NIS2-richtlijn, net zoals de NIS1-richtlijn geïmplementeerd is de Wet Beveiliging Netwerk- en Informatiesystemen. Daarmee vervangt de NIS2-richtlijn de NIS1- richtlijn. De NIS2-richtlijn bevat een uitgebreidere en explicietere beveiligingsplicht en is van toepassing op meer sectoren. Doordat de NIS2-richtlijn op meer sectoren van toepassing is dan de NIS1-richtlijn moeten meer mkb-bedrijven aan de verplichtingen van de NIS2-richtlijn voldoen. De NIS2-richtlijn kan veel impact hebben waardoor organisaties zich hier goed op moeten voorbereiden. Om organisaties te ondersteunen is een checklist ontwikkeld. Hiermee kunnen organisaties erachter komen of ze binnen het toepassingsbereik van de NIS2-richtlijn vallen. Daarnaast staat er op de checklist de verplichtingen van de NIS2-richtlijn waar organisaties die binnen het toepassingsbereik van de NIS2-richtlijn vallen aan moeten voldoen.

5.2 Centrale onderzoeksvraag

Om de ontwerpeisen van de checklist te bepalen is de volgende onderzoeksvraag ontwikkeld:

> *'Welke ontwerpeisen zijn na een analyse van de wettelijke vereisten vanuit de NIS1-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen, de NIS2-richtlijn, praktijkervaringen met betrekking tot de huidige NIS1-richtlijn en praktijkervaringen met betrekking tot de aankomende NIS2-richtlijn en het testen van een concept checklist, toepasbaar op de checklist voor het Lectoraat Juridische Aspecten van Ondernemerschap van de Hanzehogeschool Groningen?'*

5.3 Vergelijking theorie- en praktijkonderzoek

Uit zowel de ontwerpeisen van de theorie en praktijk blijkt dat cybersecurity ontzettend belangrijk wordt geacht. Dit blijkt uit de ontwerpeisen van de theorie doordat de NIS-richtlijnen er zijn voor de verbetering van de digitale en economische weerbaarheid van de Europese Lidstaten. Daarnaast zijn de NIS-richtlijnen er om cybersecurity op een verbeterd niveau te brengen en te houden. Uit de ontwerpeisen van de praktijk blijkt dat cybersecurity essentieel is voor de organisaties. De organisaties van het praktijkonderzoek vallen of binnen het toepassingsbereik van de WBNI of zijn ISO27001-gecertificeerd. Voor zowel de WBNI en ISO 27001 moet er kunnen worden aangetoond dat de netwerk- en informatiesystemen van de organisatie aan bepaalde beveiligingseisen voldoet.

Daarnaast blijkt uit de ontwerpeisen van het theoretisch onderzoek dat de implementatietermijn van de NIS2-richtlijn in oktober 2024 is. In Nederland wordt de NIS2-richtlijn geïmplementeerd in de WBNI, net zoals de implementatie van de huidige NIS1-richtlijn. Echter blijkt uit de ontwerpeisen van het praktijkonderzoek dat er een kans bestaat dat de Nederlandse implementatie niet tijdig afgerond gaat zijn. Daarnaast blijkt uit de ontwerpeisen van het praktijkonderzoek dat organisaties de Nederlandse implementatie van de NIS2-richtlijn willen afwachten voordat zij stappen gaan ondernemen. Vanuit de ontwerpeisen uit de theorie en de praktijk wordt er aangeraden om de organisatie voor te bereiden op de komst van de NIS2-richtlijn.

Vervolgens blijkt vanuit de ontwerpeisen van het theoretisch onderzoek dat de zeven sectoren van de NIS1-richtlijn ook binnen het toepassingsbereik van de NIS2-richtlijn gaan vallen. In Nederland houdt dit in dat de WBNI op dit moment van toepassing is op 350 organisaties en de verwachtingen is dat de NIS2-richtlijn op ongeveer 10.000 organisaties van toepassing gaat zijn. Uit de ontwerpeisen van het praktijkonderzoek blijkt dat het voor organisaties onduidelijk kan zijn of zij wel of niet binnen het toepassingsbereik van de NIS2-richtlijn vallen. Het gaat hier met name over de vraag of de organisatie meer dan 50 werknemers in dienst heeft en of het jaaromzet en balanstotaal meer dan 10 miljoen euro is.

Tevens blijkt uit de ontwerpeisen van zowel de theorie en praktijk dat de NIS-richtlijnen bepaalde verplichtingen met zich mee brengen, zoals de beveiligingsplicht en de meldplicht. De ontwerpeisen van het theoretisch onderzoek toont aan dat een aantal verplichtingen van de NIS1-richtlijn overeenkomen met de WBNI, maar ook dat er een aantal verschillen zijn. De beveiligingseisen van de NIS1-richtlijn zijn een open norm. In de WBNI en BBNI wordt hier iets meer duidelijkheid aangegeven door in artikel 7 en 8 van de WBNI vijf basismaatregelen voor te schrijven. In de NIS2-richtlijn worden in artikel 21 lid 2 sub a tot en met j maatregelen genoemd voor het beheer van cyberbeveiligingsrisico's. Uit de ontwerpeisen van het praktijkonderzoek blijkt dat deze beveiligingseisen voor een deel overeenkomen met de vijf basismaatregelen van de WBNI en met de beveiligingseisen van ISO 27001.

Ook blijkt uit de ontwerpeisen van het theoretisch onderzoek dat de meldplicht in de WBNI anders is dan de NIS1-richtlijn voorschrijft. Zo wordt er in de WBNI onderscheid gemaakt in de meldplicht voor 'vitale aanbieders' en 'digitale dienstverleners', terwijl dit onderscheid niet in de NIS1-richtlijn wordt gemaakt. Ook blijkt uit de ontwerpeisen van de theorie dat de drempels voor het melden van incidenten in de NIS2-richtlijn zijn verlaagd in vergelijking met de NIS1-richtlijn. Voor de NIS2-richtlijn moeten meer incidenten verplicht worden gemeld. Zo is er in beide richtlijnen een verschil in de definitie van het begrip 'incident'. Uit de ontwerpeisen van het praktijkonderzoek blijkt dat organisaties die op dit moment onder de WBNI vallen, incidentenmeldingen moeten vastleggen in een calamiteitenplan. In het calamiteitenplan staat een deels ingevulde rapportage met daarin de aard en omvang van het incident, de mogelijke gevolgen van het incident en het tijdstip wanneer het incident heeft plaatsgevonden. Uit de ontwerpeisen van het praktijkonderzoek blijkt dat de organisatie nog niet eerder te maken heeft gehad met een incident die moet worden gemeld op grond van de meldplicht. Dit wordt bevestigd in de ontwerpeisen van de theorie aangezien er in 2022 geen incidenten gerapporteerd zijn aan de toezichthouders die de drempelwaarde overschreden.

Ten slotte blijkt uit de ontwerpeisen van het theoretisch onderzoek dat er voor toezicht een verschil is tussen aanbieders van essentiële diensten en belangrijke diensten. Voor essentiële organisaties is het toezicht proactief en voor belangrijke entiteiten reactief. Uit de ontwerpeisen van de praktijk blijkt dat er in Nederland op dit moment proactief toezicht plaatsvindt voor essentiële diensten en reactief voor digitale aanbieders. Dit proactieve toezicht vindt jaarlijks plaats doormiddel van een audit die fysiek plaatsvindt op locatie van de betreffende organisatie. Bij de NIS2-richtlijn gaat dit bezoek niet altijd fysiek plaatsvinden, gezien het niet haalbaar is om fysiek langs te gaan vanwege de hoeveelheid organisaties die binnen het toepassingsbereik van de NIS2-richtlijn vallen.

5.4 Vergelijking onderzoeksobjecten praktijk

Voor het praktijkonderzoek zijn er drie verschillende organisaties geïnterviewd. Ten eerste is er een organisatie geïnterviewd die op dit moment binnen het toepassingsbereik van de WBNI valt. Ten tweede is er een organisatie geïnterviewd die op dit moment nog niet binnen het toepassingsbereik van de WBNI valt, maar wel binnen het toepassingsbereik van de NIS2-richtlijn. Tot slot is er organisatie geïnterviewd die op dit moment nog niet binnen het toepassingsbereik van de NIS2- richtlijn valt, maar als de organisatie meer dan 50 werknemers in dienst heeft dan wel. Een vergelijking uit de ontwerpeisen is dat cybersecurity voor alle drie de organisaties ontzettend belangrijk is. Een verschil in de ontwerpeisen is dat de interpretatie van voor organisaties zonder juridische kennis lastig kan zijn in tegenstelling tot organisaties met juridische kennis. Voor organisaties die op dit moment binnen het toepassingsbereik van de WBNI vallen is dit eenvoudiger aangezien deze organisaties vaak juristen in dienst hebben.

Kleinere organisaties hebben niet altijd juristen in dienst en moeten dit soort taken bijvoorbeeld uitbesteden aan externe partijen. Daarnaast is een andere ontwerpeis dat organisaties de genomen maatregelen moeten registeren, rekening houdend met de tijd en mankracht die hierbij komt kijken.

Naast de drie verschillende organisaties, heeft er ook een interview plaatsgevonden met een toezichthouder van de WBNI. Uit de ontwerpeisen van het praktijkonderzoek blijkt hoe een organisatie, die binnen het toepassingsbereik van de WBNI valt, het toezicht ervaart. Namelijk dat er jaarlijks een audit plaatsvindt door de toezichthouder en dat op basis van de audit een rapport wordt opgesteld. Uit de ontwerpeisen van het praktijkonderzoek met de toezichthouder blijkt de audit overeen te komen. Op alle essentiële entiteiten van de WBNI is er proactief toezicht aan de hand van een fysieke audit. Na de audit wordt er een rapport opgesteld met daarin de verbeterpunten voor een organisatie. Ook blijkt uit de ontwerpeisen van het praktijkonderzoek met de toezichthouder dat over het toezicht in de NIS2-richtlijn nog weinig bekend is, maar dat de toezichthouders in ieder geval een afwegingskader moeten maken over hoe het toezicht gaat plaatsvinden. Daarnaast worden bestuurders in de NIS2-richtlijn eerder verantwoordelijk gesteld.

5.5 Conclusie definitieve ontwerpeisen

Concluderend zijn dit de ontwerpeisen naar aanleiding van de analyse van de wettelijke vereisten vanuit de NIS1-richtlijn, de NIS2-richtlijn, de Wet Beveiliging Netwerk- en Informatiesystemen, praktijkervaringen met betrekking tot de huidige NIS1-richtlijn en praktijkervaringen met betrekking tot de aankomende NIS2-richtlijn, de best practice en het testen van de conceptversie van het beroepsproduct.

De eerste ontwerpeis is dat cybersecurity cruciaal is en dat dit moet worden overgedragen in de checklist. Het is belangrijk dat organisaties het belang van cybersecurity in zien en daardoor beveiligingseisen voor cybersecurity gaan toepassen binnen de organisatie. De NIS-richtlijnen kunnen worden gezien als handvatten om netwerk- en informatiesystemen beter te beveiligen. De implementatietermijn van de NIS2-richtlijn is in oktober 2024. In Nederland wordt de NIS2-richtlijn in de WBNI geïmplementeerd. Dit houdt in dat de wet- en regelgeving eind oktober 2024 van kracht is. Daaruit kan geconcludeerd worden dat organisaties die binnen het toepassingsbereik van de NIS2- richltijn vallen, eind oktober 2024, aan de verplichtingen van de NIS2-richtlijn moeten voldoen.

De tweede ontwerpeis is dat het voor organisaties duidelijk moet zijn of ze wel of niet binnen het toepassingsbereik van de NIS2-richtlijn vallen. Daarom moet op de voorkant van de checklist duidelijk worden omschreven welke stappen de organisatie moet nagaan om hier achter te komen. De eerste ontwerpeis is dat de organisatie moet nagaan of de organisatie onder één van de achttien sectoren valt. De tweede ontwerpeis is dat de organisatie moet nagaan of de organisatie in Nederland is gevestigd. De derde ontwerpeis is dat de organisatie moet nagaan of de organisatie meer dan 50 werknemers in dienst heeft en/of een jaaromzet en balanstotaal van meer dan 10 miljoen. Uiteindelijk komt de organisatie bij het resultaat of de organisatie wel of niet binnen het toepassingsbereik van de NIS2-richtlijn valt. Om deze stappen te verduidelijken wordt er via een QR- code verwezen naar een vierde ontwerpeis, namelijk de zelf-evaluatie van de Rijksoverheid. Via de zelf-evaluatie kunnen organisaties er ook achter komen of zij binnen het toepassingsbereik van de NIS2-richtlijn vallen. Via de zelf-evaluatie heeft een organisatie de mogelijkheid om per antwoord door te klikken om zo een uiteindelijk resultaat te krijgen. Daarnaast wordt in de zelf-evaluatie extra uitleg gegeven over de verschillende sectoren. Dit kan organisaties helpen om te bepalen of de organisatie wel of niet binnen de sector valt.

De vijfde ontwerpeis is dat de verplichtingen van de NIS2-richtlijn duidelijk moeten worden omschreven in de checklist, zodat organisaties hier eenvoudig gebruik van kunnen maken. Op de achterkant van de checklist staan de beveiligingseisen van de NIS2-richtlijn. De organisatie kan per beveiligingseisen afvinken aan welke beveiligingseisen de organisatie al voldoet en welke eisen nog niet. Deze beveiligingseisen komen voor een deel overeen met de ISO 27001/27002 en de WBNI. Ook voor deze organisaties is het belangrijk om na te gaan welke beveiligingseisen de organisaties al wel en nog niet hanteren. De organisaties hebben behoefte aan meer informatie per beveiligingseis. Daarom is er een zesde ontwerpeis, namelijk een QR-code die verwijst naar de pagina van Digital Society Hub met daarin extra informatie over de beveiligingseisen van de NIS2-richtlijn. Ook staat er in de uitwerking extra informatie over de meldplicht, toezicht en sancties. De beveiligingseisen worden op de pagina stuk voor stuk toegelicht in een schrijfstijl dat ook voor organisaties zonder juridische kennis duidelijk is. Hieruit vloeit ook een zevende ontwerpeis, namelijk dat de checklist ook begrijpelijk moet zijn voor organisaties met geen of weinig juridische kennis.

De verwachtingen zijn dat het registeren van de genomen maatregelen voor de NIS2-richtlijn een uitdaging gaat worden. Daarnaast kunnen de maatregelen veel tijd, mankracht en geld kosten. Hieruit vloeit de achtste ontwerpeis, namelijk om organisaties hierover te adviseren in de uitwerking van de checklist, zodat ze zich hier op kunnen voorbereiden.

Een ontwerpeis die niet wordt meegenomen in de checklist is hoe het toezicht wordt geregeld in de NIS2-richtlijn. Dit komt omdat hier op dit moment nog weinig over bekend is. Daarnaast is het toezicht ook geen verplichting van een organisatie die onder het toepassingsbereik van de NIS2- richtlijn valt. Het is daarom voor organisaties niet relevant om dit te benoemen in de checklist. Wat voor organisaties wel relevant is om te weten dat er toezicht plaatsvindt op de naleving van de NIS2- richtlijn en dat voor niet naleving sancties kunnen worden gegeven. Deze punten worden daarom wel in de ontwerpeisen van de checklist meegenomen, zodat organisaties wel op de hoogte zijn van het toezicht en dat het niet naleven van de verplichtingen van de NIS2-richtlijn consequenties kan hebben.

Aan de hand van de uitgebreide checklist kunnen organisaties snel vaststellen of ze onder de NIS2- richtlijn vallen en welke verplichtingen deze richtlijn met zich meebrengt. Zo kunnen organisaties zich goed voorbereiden en onaangename verrassingen voorkomen.

Literatuurlijst

Awesta 2020
A.G. Awesta, *de grondslagen van de cyberspace: informatiebeveiliging, privacyrecht, gegevensbescherming & cybercriminaliteit*, Deventer: Wolters Kluwer 2020.

Brouwer & Van Mil 2023
N. Brouwer & J. van Mil, 'Cybersecurity in Europa', NJB 2023/674, p. 675.

Brouwer & Reijneveld 2023
N. Brouwer & M. Reijneveld, '*de ontwikkeling van cyberveiligheid in Europa',* Nederlands Juristenblad 2023, p. 675.

Van Buuren 2023
E. van Buuren, 'Wat betekent de NIS2-richtlijn voor onze decentrale overheid?', europadecentraal.nl, 5 september.

Grotenhuis 2023
F.D.J. Grotenhuis, *Toezicht houden op ICT*, (Steekproefonderzoek Nyenrode Commissarissen Cyclus 61), 2023.

Hoekman & Hornstra 2023
P. Hoekman & A. Hornstra, *Ontwerpgericht onderzoek in de (sociaal-)juridische beroepspraktijk*, Groningen/Utrecht: Noordhoff uitgevers 2023.

Kalis 2017
J.P. Kalis, *De netwerk en informatiebeveiligingsrichtlijn*, (Universiteit Leiden), 2017.

Samenhangend Inspectiebeeld cybersecurity vitale processen 2023
Samenhangend Inspectiebeeld cybersecurity vitale processen, uitgave Rijksinspectie Digitale Infrastructuur, Uitgave Ministerie van Economische Zaken en Klimaat, Groningen, 2023.

Viergever & Van Til 2023
L. Viergever & T. van Til, 'NIS2 en de AVG: werk aan de winkel', *Computerrecht 2023,* p. 166.

Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners 2018
Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners, Uitgave Ministerie van Economische Zaken en Klimaat, Den Haag 2018.

Wondolleck & 't Hart, 2023
T.R.A. Wondolleck & E.L.V. 't Hart, 'De NIS2-richtlijn', *Nederlands Juristenblad 2023*, p. 37.

Beroepsproduct

De meldplicht van cyberincidenten binnen het Martini Ziekenhuis: Implementatie en handhaving

Maaike Mast

Samenvatting

Dit onderzoek richtte zich op het ontwerpen van een procedurebeschrijving voor de meldplicht van cyberincidenten binnen het Martini Ziekenhuis (MZH), naar aanleiding van de implementatie van de NIS2-richtlijn. De NIS2-richtlijn is bedoeld om de cyberbeveiliging binnen de EU te versterken en stelt eisen aan organisaties om significante incidenten te melden die daadwerkelijk of potentieel schade kunnen veroorzaken. Het doel van het onderzoek was om een procedurebeschrijving te ontwikkelen die zowel voldoet aan de wettelijke eisen als praktisch bruikbaar is voor alle afdelingen binnen het ziekenhuis (bijlage 1).

Het onderzoek werd uitgevoerd tussen 9 september 2024 en 10 januari 2025, in nauwe samenwerking met interne betrokkenen, waaronder functionarissen zoals de Functionaris Gegevensbescherming (FG) ende Chief Information Security Officer (CISO).

De centrale onderzoeksvraag luidde:
Welke ontwerpeisen zijn, na een analyse van de uit de NIS 2- richtlijn voortvloeiende verplichtingen voor cyberincident meldingen binnen zorginstellingen, relevante wet- en regelgeving, vakliteratuur op het gebied van informatiebeveiliging, kennis en ervaringen van interne betrokkenen binnen het Martini Ziekenhuis, en feedback op de procedurebeschrijving, relevant voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis?

Om deze vraag te beantwoorden, is gebruikgemaakt van een combinatie van theoretisch en praktijkgericht onderzoek.

Onderzoeksmethoden

Er zijn relevante wetten en richtlijnen zoals de NIS2-richtlijn, AVG en NEN7510 geanalyseerd. Daarnaast zijn interviews en feedbacksessies gehouden met interne betrokkenen, zoals de Functionaris Gegevensbescherming (FG), de Chief Information Security Officer (CISO), en andere betrokkenen. De praktijkgerichte interviews werden gehouden met in totaal 6 deelnemers, waaronder technisch en niet-technisch personeel, management en

IT-experts. Daarnaast werden de feedbacksessies georganiseerd met de Functionaris Gegevensbescherming en de CISO van het Martini Ziekenhuis. De verzamelde feedback heeft geleid tot belangrijke aanpassingen in de procedurebeschrijving, zoals het toevoegen van een heldere definitie van “significant incident” en het opnemen van bijna-incidenten. Het onderzoek benadrukt dat de procedure begrijpelijk moet zijn voor zowel technisch als niet-technisch personeel. Daarom zijn technische termen toegelicht, en is een overzichtelijke indeling gekozen met duidelijke verantwoordelijkheden en stappen.

Belangrijkste resultaten

Theoretische eisen: Uit de theoretische analyse bleek dat de NIS2-richtlijn een meldplicht voorschreef voor incidenten met daadwerkelijke of potentiële schade, inclusief vroege waarschuwingen binnen 24 uur en een opvolging binnen 72 uur. De AVG legde nadruk op de bescherming van persoonsgegevens en vereiste melding van datalekken. De NEN7510 stelde daarnaast technische beveiligingseisen die specifiek gericht zijn op de zorgsector.
Praktische inzichten: De praktijkanalyse toonde aan dat interne betrokkenen, zoals de Privacy Officer, CISO, TSO en Service Manager ICT, het belang benadrukten van heldere verantwoordelijkheden, eenvoudige taal in de procedure en concrete stappenplannen.
Bijna - incidenten werden als essentieel toegevoegd aan de meldplichtprocedures, omdat deze bijdroegen aan een completer dreigingsbeeld van cyberincidenten. Feedbacksessies benadrukten bovendien dat de procedurebeschrijving toegankelijk en begrijpelijk moest zijn, met duidelijke criteria voor significante incidenten en eenvoudigere terminologie. Deze elementen dragen bij aan de bruikbaarheid van de procedurebeschrijving binnen niet-technische afdelingen.

Het beroepsproduct

Het eindproduct van het onderzoek, een procedurebeschrijving voor de meldplicht van cyberincidenten binnen het Martini Ziekenhuis Groningen, integreerde zowel juridische als praktische eisen. Het document biedt:

- Duidelijke verantwoordelijkheden en bevoegdheden.
- Een stappenplan voor incidentmeldingen, inclusief bijna-incidenten.
- Toegankelijke taal en uitleg van technische termen.
- Compliance met de NIS2-, AVG- en NEN7510-eisen.

De procedurebeschrijving werd ontworpen om te worden opgenomen in de interne richtlijnen van het Martini Ziekenhuis om te dienen als standaard voor het omgaan met de meldplicht van cyberincidenten in de dagelijkse praktijk (bijlage 1).

Conclusie

Het onderzoek heeft geleid tot een duidelijke procedurebeschrijving waarmee het Martini Ziekenhuis voldoet aan de eisen van de NIS2-richtlijn. De procedure is praktisch en gemakkelijk toepasbaar. Dankzij het toegankelijke ontwerp is er een stabiel en toekomstgericht systeem ontwikkeld voor het beheren van de meldplicht van cyberincidenten. Dit versterkt de digitale veiligheid binnen het ziekenhuis en biedt een goede basis voor het omgaan met mogelijke cyberdreigingen.

1. Inleiding

1.1 Inleiding

Dit hoofdstuk beschrijft de context en achtergrond van het onderzoek naar de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis (MZH), uitgevoerd naar aanleiding van de implementatie van de NIS2-richtlijn. De NIS2-richtlijn, bedoeld om de cyberbeveiliging binnen de EU te versterken, introduceert strengere eisen voor risicobeheer, meldprocedures en samenwerking. Het onderzoek wordt uitgevoerd op de ICT-(BAS) afdeling en wordt begeleid door de Functionaris Gegevensbescherming (FG). De opdrachtgever, het Martini Ziekenhuis in Groningen, biedt specialistische zorg met een focus op kwaliteit, patiëntgerichtheid en innovatie. De vraagstukken richten zich op het ontwikkelen van een procedure voor cyberincidentmeldingen die voldoen aan de nieuwe regelgeving en aansluiten bij de bestaande structuur en behoeften van het MZH. Aan de hand van de onderzoeksvragen wordt gekeken hoe deze procedure vormgegeven moet worden, welke wettelijke kaders daarbij relevant zijn en hoe inzichten uit vakliteratuur en praktijkonderzoek kunnen bijdragen aan een effectieve implementatie. Het doel is een procedurebeschrijving die bruikbaar is voor alle afdelingen en bijdraagt aan de cyberweerbaarheid van het MZH.

1.2 De opdrachtgever

1.2.1 De organisatie

Opdrachtgever voor dit onderzoek is het Martini Ziekenhuis in Groningen, een toonaangevend algemeen ziekenhuis dat hoogwaardige specialistische medische zorg biedt.
Martini Ziekenhuis, gevestigd in Groningen, Nederland, is een uitgebreid algemeen ziekenhuis dat een breed scala aan gespecialiseerde medische diensten aanbiedt, van eerstelijnszorg tot zeer gespecialiseerde behandelingen. Naast curatieve zorg biedt Martini Ziekenhuis diagnostische diensten en preventieve zorg. Het ziekenhuis, hierna te noemen MZH, richt zich sterk op patiëntgerichte zorg, kwaliteit en innovatie in de gezondheidszorg.[1]De kernactiviteiten bij MZH omvatten een verscheidenheid aan medische specialismen die gericht zijn op het

1 ‘Ziekenhuizen, Martini Ziekenhuis’, ziekenhuischeck.nl.

leveren van patiëntgerichte gezondheidszorgdiensten met een focus op continue verbetering en innovatie.[2]

1.2.2 Functie en afdeling

De praktijkbegeleider voor dit onderzoek is de Functionaris Gegevensbescherming (FG), verantwoordelijk voor het toezicht op de naleving van de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Deze rol omvat het toezicht houden op gegevensverwerkingsactiviteiten, adviseren over privacykwesties en het dienen als aanspreekpunt voor zowel betrokkenen (zoals patiënten) als de Autoriteit Persoonsgegevens (AP).[3]
Het onderzoek wordt uitgevoerd binnen de ICT-BAS (Beleid, Advies en Service) afdeling, die onderdeel is van de ICT-afdeling van MZH. Hoewel deze afdeling verantwoordelijk is voor het beheer en de ondersteuning van de kern-IT infrastructuur, moet het eindproduct van dit onderzoek toepasbaar zijn in het hele ziekenhuis, zodat bruikbaarheid in alle afdelingen gewaarborgd is.

1.3 Het vraagstuk

1.3.1 Aanleiding

Dit onderzoek wordt uitgevoerd naar aanleiding van de implementatie van de NIS2-Richtlijn (Network and Information Security). Deze richtlijn moet worden omgezet naar nationale wetgeving. De NIS2- richtlijn is een Europese richtlijn die gericht is op het versterken van de cyberbeveiliging binnen de Europese Unie. Deze richtlijn, officieel bekend als de Richtlijn inzake maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, is de opvolger van de oorspronkelijke NIS- richtlijn die in 2016 werd geïmplementeerd.[4]

Een richtlijn is een juridisch instrument van de Europese Unie (EU) dat bindend is voor de lidstaten met betrekking tot het te bereiken resultaat, maar de lidstaten hebben de vrijheid om zelf te bepalen hoe ze dit resultaat bereiken. Dit betekent dat elke lidstaat de richtlijn moet omzetten in nationale wetgeving binnen een bepaalde termijn, maar zij mogen zelf kiezen op welke manier dit gebeurt, zolang het uiteindelijke doel van de richtlijn wordt bereikt.[5]
Het doel van de NIS 2-richtlijn is om een hoger niveau van cyberbeveiliging te waarborgen binnen de EU, rekening houdend met de toenemende digitale dreigingen. De richtlijn is ontworpen om de weerbaarheid van kritieke infrastructuren te vergroten en de reactie op cyberincidenten te verbeteren.[6]

De NIS 2-richtlijn moet door de EU-lidstaten in nationale wetgeving worden omgezet, en organisaties binnen de scope van de richtlijn moeten voldoen aan de gestelde eisen om sancties te voorkomen.[7]

2 ‘Kwaliteit en onderzoek’,martiniziekenhuis.nl.
3 ‘Over de autoriteit persoonsgegevens’, autoriteitpersoonsgegevens.nl.
4 ‘NIS2-Richtlijn’, digitaleoverheid.nl.
5 ‘Soorten rechtshandelingen’, european-union.europa.eu.
6 Artikel 1, eerste lid, en de overwegingen 4 en 5 NIS2-richtlijn.
7 ‘NIS2-Richtlijn’, digitaleoverheid.nl.

De Europese datum voor de implementatie van de NIS 2-richtlijn is vastgesteld op 17 oktober 2024. Voor deze datum moeten alle EU-landen de nieuwe inhoud van de NIS2 richtlijn omzetten in nationale wetgeving. Op deze datum moet de richtlijn in alle EU-landen in de nationale wetgeving zijn opgenomen, al kunnen de tijdlijnen en procedures per land verschillen.
Wanneer Nederland een EU- richtlijn niet binnen de vastgestelde termijn in nationale wetgeving implementeert, heeft dit juridische gevolgen die voortvloeien uit het Europese recht. Nederland is verplicht om EU-richtlijnen binnen de gestelde termijn om te zetten in nationale wetgeving. Indien dit niet gebeurt, kan de Europese Commissie een inbreukprocedure starten bij het Hof van Justitie van de EU (HvJEU), wat kan leiden tot boetes en dwangsommen. Daarnaast kan een richtlijn, wanneer de implementatietermijn is verstreken, onder bepaalde voorwaarden directe werking hebben. Dit kan enkel indien de bepalingen van de richtlijn voldoende duidelijk, precies en onvoorwaardelijk zijn. In dat geval kunnen burgers en bedrijven zich beroepen op de richtlijn tegenover de overheid of overheidsinstanties. Dit wordt verticale directe werking genoemd. Richtlijnen hebben echter normaal gesproken geen horizontale directe werking, wat betekent dat particulieren en bedrijven zich niet rechtstreeks tegen elkaar kunnen beroepen op een niet-geïmplementeerde richtlijn.[8]

Bovendien zijn nationale rechters verplicht om het nationale recht zoveel mogelijk richtlijnconform te interpreteren, zelfs als de richtlijn nog niet is omgezet. Dit betekent dat de nationale wetgeving geïnterpreteerd moet worden in overeenstemming met de doelstellingen van de richtlijn, zolang dit juridisch haalbaar is. Indien het uitblijven van de implementatie leidt tot schade voor burgers of bedrijven, kan Nederland aansprakelijk worden gesteld op grond van de Francovich-doctrine. Dit vereist dat er sprake is van een schending van EU-recht door de staat, dat de schending voldoende ernstig is en dat er een direct causaal verband bestaat tussen de schending en de geleden schade.

Kortom, als Nederland een richtlijn niet tijdig in nationale wetgeving omzet, kunnen burgers en bedrijven in bepaalde gevallen rechten ontlenen aan de richtlijn. Dit is vooral het geval wanneer de richtlijn duidelijk en precies is en de implementatietermijn is verstreken. Tegelijkertijd loopt de Nederlandse overheid het risico op juridische procedures en mogelijke sancties vanuit de EU.[9]

In Nederland wordt de NIS2-richtlijn geïmplementeerd in de vorm van de Cyberbeveiligingswet. Op het moment dat de Cyberbeveiligingswet wordt aangenomen, vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni).[10]

Op dit moment bevindt de implementatie zich in de fase van wetgevingsvoorbereiding. Dit houdt in dat er wordt gewerkt aan het opstellen van de wet en het afstemmen met relevante stakeholders, waaronder overheidsinstanties, bedrijven en andere betrokken partijen.
Er zijn verschillende consultaties en bijeenkomsten georganiseerd om input van deze stakeholders te verzamelen, zodat de wetgeving effectief kan inspelen op de huidige behoeften op het gebied van cyberbeveiliging. De NIS2-richtlijn breidt de regelgeving uit naar meer

8 ‘Toepassing van EU-wetgeving’, commission.europa.eu.
9 EHRM 19 november 1991, ECLI:EU:C:1991:428 (Frankovich/Italie).
10 ‘Wat gaat de nis2-richtlijn betekenen voor uw organisatie?’, ncsc.nl.

sectoren, waaronder kritieke gebieden zoals energie, transport, bankwezen, infrastructuur, gezondheid, drinkwatervoorziening, digitale infrastructuur en digitale diensten. Organisaties binnen deze sectoren moeten striktere beveiligingsmaatregelen implementeren om een beter bestand te zijn tegen cyberdreigingen, met vereisten voor risicobeheer, beveiligingscontroles en incidentrespons. Bovendien legt de richtlijn een meldplicht op voor incidenten met grote impact en introduceert deze strengere rapportagedeadlines en hoge boetes bij niet-naleving. Om cyberbeveiliging in de EU te versterken, wordt samenwerking tussen lidstaten vergroot, met verplichtingen tot het delen van informatie en het oprichten van samengestelde incidentresponsteams. Lidstaten moeten daarnaast onafhankelijke toezichthouders aanwijzen om toezicht te houden op naleving en handhaving van de richtlijn.[11,12,13].

1.3.2 Het vraagstuk van de opdrachtgever

Het vraagstuk van de opdrachtgever ziet op de vraag hoe de meldplicht van Cyberincidenten binnen het Martini Ziekenhuis, zoals voorgeschreven in de richtlijn, kan worden vorm gegeven en gehandhaafd, en welke factoren spelen een rol bij het bepalen of een incident meldingswaardig is? Het belang van het inzichtelijk maken hoe de meldplicht van cyberincidenten voor het Martini Ziekenhuis (MZH) kan worden vormgegeven en gehandhaafd strekt zich uit tot zowel externe als interne voordelen. Door een effectief systeem voor het melden van incidenten op te zetten, verbetert het MZH de coördinatie binnen de toeleveringsketen van de gezondheidszorg, waardoor het risico wordt verkleind dat incidenten escaleren en andere belanghebbenden beïnvloeden. Deze aanpak versterkt een collectieve respons binnen het netwerk van zorgverleners, leveranciers en bijbehorende partijen. Intern is het verzekeren van naleving van de vereisten voor incidentenrapportage gunstig voor patiënten, omdat het hun gevoelige informatie beschermt en hun vertrouwen in de instelling behoudt. Deze proactieve houding verlicht ook stress en onzekerheid onder ziekenhuispersoneel en management, die duidelijkheid krijgen over hun rol in incidentmanagement. Het verwaarlozen van deze verantwoordelijkheden kan het MZH daarentegen blootstellen aan financiële boetes, reputatieschade en potentiële beperkingen. Tot op heden heeft MZH vertrouwd op bestaande beleidslijnen en protocollen die zijn vormgegeven door de huidige wettelijke kaders. Gerichte maatregelen die specifiek aansluiten bij de mandaten van de NIS2-richtlijn, moeten nog worden geïmplementeerd. Deze opdracht is daarom gericht op het ontwikkelen van een duidelijke en efficiënte procedure voor het melden van cyberincidenten in overeenstemming met de NIS2-normen, waardoor het MZH kan voldoen aan de wettelijke vereisten en zijn verdediging tegen cyberincidenten kan versterken.

1.4 Het beroepsproduct

Er is gekozen voor een procedurebeschrijving als beroepsproduct, waarin de benodigde stappen en acties voor naleving van de meldplicht van de NIS2-richtlijn worden beschreven. Deze procedure is bedoeld om de tijdige melding van incidenten aan regelgevende instanties te vergemakkelijken en tegelijkertijd de vertrouwelijkheid en veiligheid van patiëntgegevens te waarborgen.

11 Viergever & van Til 2023.
12 Van Aardenne & Barensen 2023, p. 78-81.
13 Richtlijn (EU) 2022/2555.

De noodzaak om deze procedure te ontwikkelen, komt voort uit meerdere kritische factoren. Ten eerste verplicht de NIS2-richtlijn het melden van significante cyberincidenten, en een duidelijke procedure zal het MZH helpen om effectief aan deze wettelijke vereisten te voldoen. Bovendien biedt de procedure een gestructureerde aanpak voor het beheren van cyberdreigingen, waardoor risico's voor patiëntgegevens en de activiteiten van het ziekenhuis worden geminimaliseerd. Het weergeven van dit proces in een gemakkelijk te begrijpen format zal de consistente implementatie in alle afdelingen verder ondersteunen, waardoor wordt verzekerd dat de meldplicht uniform wordt begrepen en toegepast. De initiële ontwerpvereisten voor deze procedure werden geïdentificeerd door voorbereidende vergaderingen metde ICT-teamleider en de Functionaris Gegevensbescherming. Deze omvatten een focus op duidelijkheid en toegankelijkheid, het verzekeren dat de inhoud beknopt en visueel aantrekkelijk is, het gebruik van korte zinnen, opsommingstekens en relevante pictogrammen. De procedure moet ook bruikbaar zijn voor alle afdelingen, waardoor het gemakkelijk te begrijpen is voor zowel technisch als niet-technisch personeel. Ten slotte moet het document voldoen aan externe standaarden, voldoen aan de verwachtingen van regelgevende instanties en auditors, en zo een betrouwbaar kader creëren voor het melden van cyberincidenten binnen het ziekenhuis.

1.4.1 Relevante wet- en regelgeving

Bij de ontwikkeling van de procedure worden verschillende belangrijke wettelijke kaders zorgvuldig overwogen om volledige naleving te garanderen. Deze omvatten de Wet beveiliging netwerk- en informatiesystemen (Wbni),[14] de Nederlandse wetgeving die de oorspronkelijke NIS-richtlijn implementeert, en de bijgewerkte NIS2-richtlijn, die uitgebreidere cybersecurityvereisten introduceert, waaronder strengere rapportage- en beveiligingsmaatregelen. Daarnaast spelen de Algemene verordening gegevensbescherming (AVG)[15] ende Uitvoeringswet (UAVG), een cruciale rol, omdat ze de bescherming van persoonsgegevens reguleren - een cruciaal aspect voor zorginstellingen die gevoelige patiëntinformatie beheren. Tot slot biedt de NEN7510-norm, de Nederlandse informatiebeveiligingsnorm voor de gezondheidszorg, aanvullende richtlijnen voor het beschermen van gevoelige gegevens binnen ziekenhuizen. Deze kaders vormen samen de noodzakelijke wettelijke basis voor de procedure en zorgen ervoor dat MZH voldoet aan zowel nationale als Europese normen voor cybersecurity en gegevensbescherming.

1.4.2 Eerder onderzoek

Een vooronderzoek uitgevoerd binnen de HBO Kennisbank heeft meerdere studies geïdentificeerd die ingaan op de implementatie van de NIS2-richtlijn. Deze studies benadrukken specifiek de urgentie en noodzaak voor zorginstellingen om te voldoen aan de nieuwe regelgeving en hun cybersecuritymaatregelen te versterken. In dit verband biedt een checklist, ontwikkeld door een student in het kader van het Cybersecurity Noord-Nederland-project, een waardevol hulpmiddel.Deze checklist fungeert als een praktisch raamwerk dat kan dienen als uitgangspunt of richtlijn bij het ontwerpen van een procedure om aan de eisen van de NIS2-richtlijn te voldoen.[16]

14 *Kamerstukken II* 2021/22, 36084, nr 3, (MvT).
15 *Kamerstukken II* 2017/18, 34851, nr 3, (MvT).
16 Veenstra, 'Nis2 checklist', hbo-kennisbank.nl, 2024.

1.5 Onderzoeksdoelstelling

Het doel van dit onderzoek is het opleveren van een procedurebeschrijving aangaande de meldplicht van cyberincidenten voor het Martini Ziekenhuis, dat voldoet aan de vereisten voortvloeiend uit de NIS 2-richtlijn en aanverwante wet- en regelgeving omtrent cyberincident meldingen, rekening houdt met inzichten uit vakliteratuur op het gebied van informatiebeveiliging, is afgestemd op een analyse van de factoren die een rol spelen bij het bepalen of een incident meldingswaardig is binnen het ziekenhuis en rekening houdt met feedback op (en een kritische reflectie daarop) het concept van de procedurebeschrijving.

1.6 Centrale onderzoeksvraag

Welke ontwerpeisen zijn, na een analyse van de uit de NIS 2-richtlijn voortvloeiende verplichtingen voor cyberincident meldingen binnen zorginstellingen, relevante wet- en regelgeving, vakliteratuur op het gebied van informatiebeveiliging, kennis en ervaringen van interne betrokkenen binnen het Martini Ziekenhuis, en feedback op de procedurebeschrijving, relevant voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis?

1.7 Deelvragen

1.7.1 Theorie deelvragen

Welke ontwerpeisen voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis zijn relevant in het kader van de aankomende wet- en regelgeving die voortvloeit uit de NIS2-richtlijn omtrent cyberincident meldingen voor het Martini Ziekenhuis?

Welke ontwerpeisen voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis kunnen worden afgeleid uit vakliteratuur op het gebied van wettelijke verplichtingen rond de bescherming van persoonsgegevens en regels en procedures die wettelijk zijn vastgelegd voor het melden en afhandelen van cyberincidenten?

1.7.2 Praktijk deelvragen

Welke ontwerpeisen voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis zijn af te leiden uit de kennis en ervaring van interne betrokkenen, relevant t.a.v. het onderwerp, op het gebied van cyberveiligheid en de implementatie van de verplichtingen voortvloeiend uit de NIS2-richtlijn voor het Martini Ziekenhuis?

Welke ontwerpeisen voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis zijn af te leiden uit een feedbacksessie van het concept procedurebeschrijving met het personeel, IT-experts en management van het ziekenhuis?

2. Methodologische verantwoording

2.1 Inleiding

In dit hoofdstuk wordt de methodologische basis van het onderzoek uiteengezet. Het biedt een overzicht van de gebruikte theoretische bronnen, onderzoeksmethoden en de verwerking van resultaten. Door deze methodologische verantwoording wordt inzicht gegeven in de keuzes die zijn gemaakt om de onderzoeksvragen te beantwoorden en het beroepsproduct te ontwikkelen. Allereerst wordt stilgestaan bij de theoretische bronnen die zijn geraadpleegd. Deze bronnen bieden een stevig fundament voor de juridische en technische aspecten van het onderzoek. Daarnaast worden de gehanteerde onderzoeksmethoden beschreven, zoals interviews met betrokkenen en feedbacksessies. Vervolgens wordt toegelicht hoe de verzamelde informatie is verwerkt en geïntegreerd in het definitieve beroepsproduct. Hierbij is aandacht besteed aan de balans tussen juridische naleving, praktische toepasbaarheid en organisatorische implementatie. Het hoofdstuk sluit af met een reflectie op de kwaliteiten en beperkingen van zowel het onderzoek als het beroepsproduct, waarbij suggesties voor toekomstige verbeteringen worden gedaan.
Met deze methodologische verantwoording wordt een transparant beeld geschetst van de stappen die zijn genomen om een goed onderbouwde en uitvoerbare procedurebeschrijving te ontwikkelen voor de meldplicht van cyberincidenten binnen het Martini Ziekenhuis.

2.2 Theoretische bronnen theorieonderzoek

2.2.1 Literatuur (boeken en juridische tijdschriften)

Inleiding

Voor dit onderzoek is gebruik gemaakt van verschillende betrouwbare en actuele literatuur om een volledig en gedetailleerd inzicht te krijgen in de implementatie van de NIS2-richtlijn en de relevantie van de Algemene Verordening Gegevensbescherming (AVG). Een van de belangrijkste databases die is geraadpleegd, is Kluwer InView. Deze juridische database biedt uitgebreide toegang tot wet- en regelgeving, juridische tijdschriften, en boeken. De keuze voor deze bronnen is gebaseerd op hun betrouwbaarheid en uitgebreide juridische analyses, die essentieel zijn voor het begrijpen van complexe wetgeving en richtlijnen. De keuze voor Kluwer InView is gebaseerd op haar vermogen om complexe wetgeving, zoals de NIS2-richtlijn en de

AVG, diepgaand te belichten. Om relevante bronnen te vinden, is gezocht op kernbegrippen zoals “NIS2”, “Cyberbeveiliging”, “AVG”, “Meldplicht NIS2”, “Datalekken”, “Cybersecurity”. Deze zoekstrategie heeft geleid tot de selectie van boeken en artikelen die een belangrijke bijdrage hebben geleverd aan de theoretische onderbouwing van dit onderzoek. Op basis van de bevindingen uit deze bronnen wordt in de volgende sectie een overzicht gegeven van de literatuur die is gebruikt.

Van Aardenne & Barensen 2023
Bron: *H. van Aardenne & J. Barensen, ‘NIS2: nieuwe regels tegen cyberaanvallen’, Adv.bl. 2023/2041, afl. 5, p. 78-81. Dit artikel is gekozen omdat het actuele en relevante informatie biedt over de specifieke regels die de NIS2-richtlijn introduceert om cyberaanvallen tegen te gaan. Het artikel bespreekt* zowel de juridische achtergrond als de praktische toepassing van deze nieuwe richtlijn. Dit maakt het een essentiële bron voor een goed begrip van de impact van de NIS2-richtlijn op nationale wetgeving en cybersecuritymaatregelen.
Het tijdschrift waarin dit artikel is gepubliceerd, het Advocatenblad, staatbekend om zijn inhoudelijke kwaliteit en zijn relevante bijdragen aan juridische vraagstukken. Hierdoor is het een betrouwbare bron die uitstekend aansluit bij de juridische focus van het onderzoek. Het artikel biedt daarnaast een actuele analyse van de invoering van de NIS2-richtlijn, wat helpt bij het begrijpen van de uitdagingen en mogelijkheden voor implementatie in de Nederlandse context.

Brouwer & Van Mil 2023
Bron: *N. Brouwer & J. van Mil, ‘Cybersecurity in Europa’, NJB 2023/674, afl. 10, p. 748-757. Deze* bron is gekozen omdat het een uitgebreide analyse biedt van de stand van zaken rondom cybersecurity in Europa. Het artikel bespreekt hoe Europese regelgeving, inclusief richtlijnen zoals de NIS2, wordt toegepast en wat de juridische en praktische gevolgen hiervan zijn. Het is relevant voor het onderzoek vanwege zijn focus op de bredere Europese context en de praktische implicaties daarvan.

Gal-Or & Ghose 2005
Bron: *E. Gal-Or & A. Ghose, ‘The economic incentives for sharing security information’, Inform Syst Res 2005, p. 186–208. Dit artikel is geselecteerd omdat het inzicht biedt in de economische* prikkels en uitdagingen van het delen van informatie over cyberbeveiliging. Het legt een belangrijke theoretische basis voor de analyse van samenwerking en informatie-uitwisseling tussen organisaties. Dit is relevant voor het onderzoek naar de implementatie van richtlijnen zoals de NIS2, die dergelijke samenwerking stimuleren.

Gordon, Loeb & Lucyshyn 2003
Bron: *L. Gordon, M. Loeb & W. Lucyshyn, ‘Sharing information on computer systems security: an economic analysis’, J Account Public Pol 2003, p. 461–485. Deze bron is* belangrijk vanwege zijn economische analyse van informatie-uitwisseling op het gebied van computersystemen. Het artikel biedt een theoretisch kader dat helpt om de financiële en beleidsmatige aspecten van cybersecuritymaatregelen te begrijpen, wat essentieel is voor het onderzoek naar richtlijnen zoals de NIS2.

Jacobs & Jansen 2024
Bron: *B.P.F. Jacobs & R.H.T. Jansen, ‘Hoe hackers vastlopen’, Computerrecht 2024/3, afl. 1, p. 15-17. Dit* artikel is gekozen omdat het praktische inzichten biedt in hoe cybersecuritymaatregelen effectief kunnen worden toegepast om hackers tegen te werken. Het artikel is relevant vanwege de combinatie van juridische en technische inzichten, die nuttig zijn voor het onderzoek naar de implementatie van de NIS2-richtlijn.

Kranenborg & Verhey 2023
Bron: *H.R. Kranenborg & L.F.M. Verhey, ‘Melding ‘Datalekken’’, SBR Wetenschap 2024/11.5.2, p. 11. Dit artikel is geselecteerd omdat het zich richt op de meldplicht bij datalekken, een essentieel onderdeel* van de NIS2-richtlijn. Het artikel biedt inzicht in de juridische verplichtingen en praktische uitdagingen rondom datalekmeldingen, wat direct relevant is voor het onderzoek.

Praat 1998
Bron: *J.C. van Praat, ‘Information Tehtnologies Infrastucture Libary (ITIL)’, Handboek EDP-Auditing, 1998, Par. 3.6.2. Dit* boek is gekozen omdat het de uitleg geeft over de ITIL methode welke al door de FG van het ziekenhuis wordt gebruikt en gebruikt kan worden bij de meldprocedure van de NIS2- richtlijn.

Steenbrugge 2024
Bron: *W. Steenbrugge, ‘Internetconsultatie Cyberbeveiligingswet’, Computerrecht 2024/144, p. 302. Deze bron is gekozen vanwege de* focus op de Nederlandse Cyberbeveiligingswet en hoe deze aansluit bij de NIS2-richtlijn. Het artikel bespreekt de consultatiefase en de potentiële impact van de wetgeving, wat belangrijk is voor de analyse van nationale implementatie van Europese regelgeving.

Viergever & Van Til 2023
Bron: *L. Viergever & G. van Til, ‘NIS2 en de AVG’, Computerrecht 2023/116. Dit* artikel is relevant omdat het ingaat op de relatie tussen de NIS2-richtlijn en de Algemene Verordening Gegevensbescherming (AVG). Het artikel biedt belangrijke inzichten in hoe beide regelingen elkaar aanvullen en hoe organisaties aan beide verplichtingen kunnen voldoen.

2.2.2 Relevante wet- en regelgeving

Inleiding
Voor het verkrijgen van een volledig en betrouwbaar beeld van de juridische kaders rondom de NIS2- richtlijn en de Algemene Verordening Gegevensbescherming (AVG) is gebruik gemaakt van zowel Europese als nationale juridische databanken. EUR-Lex fungeerde als de primaire bron voor Europese wetgeving en richtlijnen. Dit platform biedt directe toegang tot officiële EU-documenten, wat handig is voor het verzamelen van authentieke en actuele informatie over onder meer de oorspronkelijke NIS-richtlijn, de NIS2-richtlijn en de AVG. De keuze voor EUR-Lex is gebaseerd op de betrouwbaarheid en juridische precisie van deze database, die noodzakelijk zijn om een correcte interpretatie van de Europese regelgeving te waarborgen. Naast EUR-Lex is ook wetten.overheid.nl geraadpleegd, de Nederlandse databank voor nationale wet- en regelgeving. Dit platform biedt waardevol inzicht in hoe Europese richtlijnen,

in de Nederlandse wetgeving zijn opgenomen en geïmplementeerd. Door beide databanken te combineren, werd een compleet overzicht verkregen van zowel de Europese als de nationale juridische kaders die relevant zijn voor dit onderzoek. Op basis van deze databanken is de volgende wet- en regelgeving gebruikt bij het onderzoek.

NIS en NIS2-richtlijn
De NIS-richtlijn en diens opvolger, de NIS2-richtlijn, zijn gekozen omdat deze de belangrijkste EU- regelgeving vormen voor de beveiliging van netwerk- en informatiesystemen. De NIS2-richtlijn introduceert striktere eisen en bredere toepassingsgebieden, wat van grote invloed is op hoe lidstaten en organisaties cybersecuritystrategieën ontwikkelen en uitvoeren. De NIS2-richtlijn is natuurlijk het hoofdonderwerp van het onderzoek en de oorspronkelijke richtlijn is relevant om de veranderingen aan te kunnen tonen.

AVG (Algemene Verordening Gegevensbescherming)
De AVG is opgenomen vanwege de belangrijke rol die deze speelt in de bescherming van persoonsgegevens in de EU. Omdat cybersecurity vaak hand in hand gaat met gegevensbescherming, biedt de AVG een kader dat essentieel is voor organisaties om zowel gegevensbeveiliging als wettelijke naleving te waarborgen.

UAVG (Uitvoeringswet AVG)
De UAVG is de nationale implementatiewet van de AVG in Nederland en is gekozen omdat deze verdere specificaties en richtlijnen bevat over hoe de AVG wordt toegepast binnen de Nederlandse context. Dit biedt waardevolle inzichten in hoe Nederlandse organisaties hun cybersecurity en gegevensbescherming kunnen combineren om aan beide regelgevingen te voldoen.

WBNI (Wet beveiliging netwerk- en informatiesystemen)
De WBNI is de huidige Nederlandse implementatie van de NIS-richtlijn en is relevant omdat deze wetgeving bepalend is voor de beveiliging van netwerk- en informatiesystemen in vitale sectoren. De WBNI is cruciaal voor het begrijpen van hoe Nederland cybersecurityverplichtingen vanuit de EU vertaalt in nationale wetgeving, en hoe dit handhaving en naleving beïnvloedt.

DORA (Digital Operational Resilience Act)
DORA is gekozen omdat het een nieuwe EU-verordening is die zich richt op de digitale operationele veerkracht van financiële instellingen. Deze wetgeving is relevant omdat ze een uniform kader biedt voor het omgaan met cyberrisico's en incidenten in de financiële sector, wat directe implicaties heeft voor cybersecuritymaatregelen en compliance-eisen binnen deze industrie.

BSI (Bundesamt für Sicherheit in der Informationstechnik)
Het BSI, het Duitse federale bureau voor informatiebeveiliging, is gekozen vanwege zijn toonaangevende rol in het ontwikkelen van standaarden en richtlijnen voor cybersecurity. Het BSI wordt internationaal erkend en biedt waardevolle casestudy's en richtlijnen die kunnen worden vergeleken met de Nederlandse benadering van cybersecurity.

EUR-Lex
EUR-Lex wordt gebruikt als primaire database voor Europese wetgeving en richtlijnen. Dit platform biedt directe toegang tot officiële EU-documenten, wat cruciaal is voor het verkrijgen van authentieke en actuele informatie over de oorspronkelijke NIS-richtlijn, NIS2-richtlijn en AVG. EUR-Lex werd gekozen vanwege de betrouwbaarheid en de juridische precisie, wat nodig was om correcte interpretaties van deze Europese regelgeving te kunnen rechtvaardigen.

2.2.3 Relevante internetbronnen

Inleiding
Voor dit onderzoek zijn verschillende internetbronnen geraadpleegd om een volledig inzicht te krijgen in de juridische, praktische en beleidsmatige aspecten rondom de NIS2-richtlijn en de Algemene Verordening Gegevensbescherming (AVG). De website van de Autoriteit Persoonsgegevens (AP) speelde een cruciale rol bij het bieden van inzicht in de handhaving en interpretatie van de AVG in Nederland. De actuele standpunten en richtlijnen van de AP boden waardevolle context voor de praktische implicaties van zowel de AVG als de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Daarnaast werd Overheid.nl gebruikt als centrale bron voor Nederlandse wetgeving en overheidsinformatie. Dit platform bood toegang tot de Nederlandse implementatiewetten die relevant zijn voor de NIS2-richtlijn en de AVG, wat essentieel was voor het begrijpen van de nationale vertaling en toepassing van Europese richtlijnen. Op Europees niveau bood de website van ENISA (European Union Agency for Cybersecurity) belangrijke inzichten in cyberdreigingen en beveiliging. De uitgebreide rapporten van ENISA, zoals de jaarlijkse Threat Landscape, schetsen de bredere context waarin de NIS2-richtlijn functioneert en belichten de trends en uitdagingen in de Europese aanpak van cybersecurity. De website van het Nationaal Cyber Security Centrum (NCSC) leverde waardevolle informatie over richtlijnen, adviezen en waarschuwingen met betrekking tot cybersecurity in Nederland. Het NCSC fungeert als een essentiële schakel tussen beleid en praktijk en biedt organisaties ondersteuning bij het verbeteren van hun cyberweerbaarheid in lijn met de NIS2-richtlijn. Daarnaast leverde de website van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) relevante informatie over cybersecuritybeleid in Nederland. Deze bron werd gekozen vanwege haar expertise op het gebied van nationale veiligheid en cyberdreigingen. De details van de NCTV waren essentieel om het bredere veiligheidskader waarin de NIS2-richtlijn wordt toegepast, te begrijpen. Via Google zijn de bronnen aan bod gekomen door gebruik te maken van specifieke zoektermen. Voor de Autoriteit Persoonsgegevens is gezocht op "Autoriteit Persoonsgegevens AVG richtlijnen" of "AP UAVG handhaving". Voor Overheid.nl zijn zoektermen als "Overheid.nl NIS2 richtlijn" of "Nederlandse implementatie AVG" gebruikt. Bij het vinden van informatie van ENISA is gezocht op "ENISA Threat Landscape 2023" of "ENISA NIS2 cyberbeveiliging". Voor het Nationaal Cyber Security Centrum (NCSC) zijn termen gebruikt als "NCSC NIS2 richtlijn" of "NCSC cybersecurity richtlijnen Nederland". Voor de NCTV zijn zoektermen zoals "NCTV cybersecuritybeleid" of "NCTV NIS2 veiligheid" gebruikt. Deze gerichte zoekopdrachten leiden vrijwel direct naar relevante pagina's of documenten van de genoemde bronnen. Op basis van deze internetbronnen zijn de volgende bronnen relevant voor het onderzoek.

Cybersecuritybeeld Nederland 2023
'Cybersecuritybeeld Nederland', www.nctv.nl, 2023.
Dit rapport biedt een actueel overzicht van de staat van cybersecurity in Nederland. Het bespreekt trends, dreigingen en uitdagingen, wat cruciaal is voor het begrijpen van het bredere kader waarin de NIS2-richtlijn en andere regelgevingen worden geïmplementeerd.

Nctv 2024
Nctv, nis2-richtlijn, 2024 www.nctv.nl.
Deze bron biedt een Nederlandse kijk op de implementatie van de NIS2-richtlijn en de impact daarvan op organisaties. Wat relevant is voor het onderzoek om de verandering in de richtlijn in kaart te brengen.

Welke sectoren vallen onder de NIS2-richtlijn 2024
'Welke sectoren vallen onder de NIS2-richtlijn', www.nctv.nl, 2024.
Deze bron geeft duidelijkheid over welke sectoren specifiek onder de reikwijdte van de NIS2-richtlijn vallen.

Fg informatie 2024
'Fg-informatie', www.autoriteitpersoonsgegevens.nl, 2024.
Deze bron gaat in op de rol van functionarissen voor gegevensbescherming (FG's), wat belangrijk is voor organisaties die zowel met de AVG als de NIS2-richtlijn te maken hebben.
Over de autoriteit persoonsgegevens 2024
'Over de autoriteit persoonsgegevens', www.autoriteitpersoonsgegevens.nl, 2024.
Deze bron biedt inzicht in de rol van de Autoriteit Persoonsgegevens, die toezicht houdt op de naleving van zowel de AVG als cybersecurityregels.

Nis2-richtlijn 2024
'nis2-richtlijn', www.digitaleoverheid.nl, 2024.
Dit document beschrijft de NIS2-richtlijn en haar implementatie in Nederland, wat essentieel is voor het onderzoek naar cybersecuritywetgeving om een algemeen beeld te geven.

Overzicht van alle onderwerpen 2024
'Overzicht van alle onderwerpen/nis2-richtlijn' www.digitaleoverheid.nl, 2024.
Dit overzicht biedt een samenvatting van onderwerpen die gerelateerd zijn aan de implementatie van de NIS2-richtlijn. Het onderzoek richt zich op de meldprocedure, dit is èèn van de gerelateerde onderwerpen.

ENISA Threat landscape 2021
ENISA. 'ENISA Threat Landscape. 2021', www.enisa.europa.eu, 2021.
Dit document analyseert de belangrijkste cybersecuritydreigingen op Europees niveau. Het biedt waardevolle inzichten in de context waarin Europese richtlijnen, zoals de NIS2, zijn ontwikkeld.

Wat gaat de NIS2-richtlijn betekenen voor uw organisatie? 2024
'Wat gaat de nis2-richtlijn betekenen voor uw organisatie?', www.ncsc.nl, 2024.
Deze bron bespreekt de praktische impact van de NIS2-richtlijn op organisaties in Nederland. Dit is relevant om een beeld te creeren hoe het MZH zich zal moeten aanpassen.

IT Ausfall unikllinik Dusseldorf 2020
'IT-Ausfall an der uniklinik Dusseldorf', www.uniklinik-dusseldorf.de, 2020.
De casus van de IT-storing in de Uniklinik Düsseldorf illustreert de impact van cybersecurityincidenten op vitale sectoren, zoals de gezondheidszorg. Deze bron biedt een praktijkvoorbeeld van de noodzaak van strikte naleving van richtlijnen zoals de NIS2. Het helpt ook om de gevolgen van beveiligingsproblemen beter te begrijpen en hoe dergelijke incidenten kunnen worden voorkomen. Deze bron is ook handig voor een (mogelijk) voorbeeld scenario.

2.3 Onderzoeksmethoden en- objecten praktijkonderzoek

2.3.1 Interviews

Verantwoording
Interviews zijn gekozen als onderzoeksmethode omdat ze diepgaande informatie opleveren over de ervaringen, meningen en behoeften van de betrokkenen. Deze methode is geschikt voor het bespreken van complexe onderwerpen, zoals privacybescherming, informatiebeveiliging en meldprocedures. Door persoonlijke interactie konden inzichten worden verkregen die niet altijd via andere onderzoeksmethoden, zoals enquêtes of literatuuronderzoek, beschikbaar zijn. Het type interviews dat is gebruikt, zijn semi-gestructureerde interviews. Dit type interview biedt de flexibiliteit om dieper in te gaan op specifieke onderwerpen terwijl er een basisstructuur wordt behouden. Deze aanpak maakt het mogelijk om niet alleen gestandaardiseerde informatie te verzamelen, maar ook om ruimte te laten voor aanvullende inzichten en unieke perspectieven van de geïnterviewden. Hiermee leverden de interviews waardevolle informatie op voor het onderzoek. Voor de interviews is een algemene vragenlijst ontwikkeld die bij alle functies kon worden toegepast. Deze lijst bevatte brede vragen over verantwoordelijkheden, samenwerking, de omgang met incidenten, en het naleven van relevante wet- en regelgeving, zoals de AVG en de NIS2-richtlijn. Door een algemene vragenlijst te gebruiken, werd consistentie gewaarborgd en konden overeenkomsten en verschillen tussen de rollen binnen de organisatie beter worden geanalyseerd. Voorafgaand aan de interviews is er gekeken of er vragen waren die overgeslagen konden worden of juist specifieke vragen aangevuld. Hoewel de vragenlijst algemeen van aard was, bood deze voldoende ruimte om in te zoomen op specifieke aspecten die relevant waren voor de functie of expertise van de geïnterviewde. Hierdoor konden niet alleen de verantwoordelijkheden en uitdagingen van verschillende functies worden belicht, maar werd ook inzicht verkregen in hoe deze rollen gezamenlijk bijdragen aan het waarborgen van privacy en informatiebeveiliging. Deze gestandaardiseerde aanpak maakte het mogelijk om trends en patronen in beeld te krijgen, terwijl de flexibiliteit in de gesprekken zorgde voor aanvullende inzichten. Dit heeft bijgedragen aan een breed en gedetailleerd beeld. De vragenlijst is opgenomen als bijlage 2 van dit onderzoek.

Onderzoeksobjecten
Interviews zijn afgenomen met de volgende personen:

- **De Privacy Officer:** Om inzicht te krijgen in de naleving van de AVG, meldprocedures voor datalekken, en hoe deze in lijn worden gebracht met de WGBO en de NIS2-richtlijn.
- **De CISO:** Voor het bespreken van de technische kant van informatiebeveiliging, waaronder de toepassing van de NEN7510-normen en de praktische implementatie van cybersecuritymaatregelen.
- **De TSO:** Voor het verkrijgen van details over technische risicoanalyses, penetratietesten en het beheer van IT-beveiligingsmaatregelen.
- **De Bedrijfsjurist:** Om inzicht te krijgen in juridische verplichtingen zoals de WGBO en AVG, en hoe deze bijdragen aan het waarborgen van privacy en meldprocedures.
- **De Service Manager ICT:** Om te begrijpen hoe incidentenbeheer wordt gecoördineerd en welke rol ICT-processen spelen bij meldprocedures.
- **De Adviseur Crisisbeheersing:** Voor het bespreken van het crisismanagement bij cyberincidenten en het bespreken van scenario's en procedures die de meldplicht kunnen ondersteunen.

Onderbouwing van objecten
Deze personen zijn geselecteerd omdat zij sleutelrollen vervullen in het beheer van privacy en cybersecurity binnen het MZH. Zij zijn direct betrokken bij de implementatie van de meldplicht voor cyberincidenten en hebben unieke kennis en ervaring die van belang is voor het praktijkonderzoek. De combinatie van juridische, technische en operationele expertise biedt een compleet beeld van de huidige situatie en mogelijke verbeterpunten en wensen.

2.3.2 Feedback op concept-beroepsproduct

Verantwoording
Feedbacksessies zijn gebruikt om kwalitatieve input te verzamelen en te verwerken. Deze methode maakt het mogelijk om te beoordelen hoe het concept-beroepsproduct aansluit bij de praktijk en om verbeterpunten te identificeren. Dit helpt de haalbaarheid, bruikbaarheid en duidelijkheid van het beroepsproduct te vergroten, zodat het optimaal kan worden geïmplementeerd.

Onderzoeksobjecten
Feedback werd opgehaald bij:
De Functionaris Gegevensbescherming (FG): Om te toetsen of het beroepsproduct voldoet aan de wettelijke vereisten, zoals de AVG, en of het product aansluit bij de bredere privacydoelstellingen van het ziekenhuis. De FG fungeerde tevens als projectleider voor het onderzoek.
De CISO: Om na te gaan of het beroepsproduct aansluit bij de technische en organisatorische eisen van de NIS2-richtlijn en om te beoordelen hoe effectief de beschreven procedure kan zijn.

Onderbouwing van objecten
Deze personen zijn geselecteerd vanwege hun expertise en directe betrokkenheid bij het onderwerp. De FG, als projectleider, heeft een cruciale rol gespeeld in de coördinatie van het onderzoek en de ontwikkeling van het beroepsproduct. De CISO is nauw betrokken bij de implementatie van de NIS2- richtlijn en kan beoordelen of het product de beoogde doelstellingen ondersteunt.

Naar aanleiding van de ontvangen feedback is de verantwoording van de keuzes verder uitgewerkt. Zo kwam uit de feedback naar voren dat het belangrijk is om niet alleen de expertise van de betrokkenen te benadrukken, maar ook hoe hun input concreet is verwerkt in het beroepsproduct.

Tijdens het onderzoek is feedback opgehaald via feedbacksessies met interne stakeholders, waaronder de Functionaris Gegevensbescherming (FG), Chief Information Security Officer (CISO). Het doel van deze sessies was om het concept-beroepsproduct te toetsen op juridische correctheid, praktische toepasbaarheid en bruikbaarheid binnen verschillende afdelingen van het Martini Ziekenhuis.
Uit de feedbacksessies kwamen diverse verbeterpunten naar voren:

- De definitie van "Significant Incident" werd als te abstract beschouwd. Dit leidde tot de toevoeging van een gedetailleerdere uitleg bij de criteria voor significante incidenten en concrete voorbeelden, zoals systeemuitval en datalekken.
- De noodzaak om aandacht te besteden aan bijna-incidenten werd benadrukt. Dit
- resulteerde in de nadruk op "ongeacht of er daadwerkelijk schade is ontstaan".
- Feedback gaf aan dat betrokkenen moeite hebben met technische terminologie in het conceptdocument. Om dit te verhelpen, definities verduidelijkt en toegevoegd met eenvoudigere uitleg van complexe termen.

De feedback is systematisch gedocumenteerd in een overzicht (zie paragraaf 4.8 van hoofdstuk 4), waarin per feedbackpunt de ontvangen input, de ondernomen actie en de verantwoording van deze actie zijn opgenomen. Daarnaast is onderzocht of het beroepsproduct in de praktijk een realistisch beeld geeft van de implementatie en toepassing binnen het ziekenhuis. Feedback wees op het belang van een duidelijke koppeling tussen theoretische richtlijnen en praktische uitvoerbaarheid. Op basis hiervan zouden scenario's en trainingsrichtlijnen toegevoegd kunnen worden aan het product om medewerkers beter voor te bereiden op mogelijke incidenten. Echter is tijdens de afstudeerperiode hier geen mogelijkheid voor in verband met de gestelde deadlines. Hoewel tijdsdruk het uitvoeren van meerdere feedbackrondes belemmerde, biedt deze aanpak een transparante basis voor toekomstige aanpassingen in de procedurebeschrijving. Deze aanpak verduidelijkt hoe feedback niet alleen de kwaliteit en toepasbaarheid van het beroepsproduct heeft versterkt, maar ook een solide basis legt voor verdere doorontwikkeling na de afstudeerperiode.

2.4 Meetinstrumenten praktijkonderzoek

2.4.1 Interviewvragen

Beschrijving: De interview vragen bestonden uit open vragen die gericht waren op het verkrijgen van diepgaande inzichten van experts binnen het MZH. De vragen behandelden onderwerpen zoals de implementatie van meldprocedures, de toepassing van AVG- en NIS2-richtlijnen, en specifieke uitdagingen op het gebied van cybersecurity en privacybescherming. Aan het begin van ieder interview is er gevraagd om een uitleg van de functie en werkzaamheden.

Hoe tot stand gekomen? De vragen zijn ontwikkeld op basis van literatuuronderzoek en praktijkervaringen. Hierbij is specifiek gekeken naar wettelijke vereisten (AVG, NIS2) en relevante kaders zoals de NEN7510. Daarnaast is input verkregen van de Functionaris Gegevensbescherming (FG) en de CISO om de vragenlijst af te stemmen op de behoeften en kennis van de geïnterviewden. Zo heb ik aanbevelingen gekregen over wie te spreken en waarom deze personen van belang konden zijn voor het onderzoek. Tijdens de gesprekken ontstonden er ook vragen om aan de andere personen te stellen of is er doorverwezen naar collega's die mogelijk meer informatie konden geven over een specifieke vraag zo werden de vragen tijdens de gesprekken enigszins aangepast.

Motivatie: Interviews waren essentieel om dieper inzicht te krijgen in de praktijk en ervaringen van sleutelpersonen zoals de Privacy Officer, CISO, TSO, en andere betrokkenen. De vragen waren flexibel genoeg om contextspecifieke antwoorden te verzamelen en gestructureerd genoeg om vergelijkbare gegevens te verkrijgen.

2.4.2 Feedback

Beschrijving: Tijdens de feedbacksessies is gebruik gemaakt van een vragen over de haalbaarheid, bruikbaarheid en duidelijkheid van het concept-beroepsproduct. De feedback bevatte ruimte voor verbetering.

Hoe tot stand gekomen? De feedback is tot stand gekomen overleg met de FG en CISO en is gebaseerd op de belangrijkste succesfactoren voor effectieve meldprocedures.

Motivatie: De feedbacksessies gaven een gestructureerde manier om input te verzamelen. Dit maakte het mogelijk om specifieke verbeterpunten te identificeren en direct toe te passen in de ontwikkeling van het beroepsproduct.

2.5 Best practices

Voor het opstellen van de procedurebeschrijving voor de meldplicht van cyberincidenten binnen het Martini Ziekenhuis, heb ik gebruik gemaakt van diverse goede voorbeelden en best practices. Deze voorbeelden hebben gediend als referentiepunten om een procedure te ontwikkelen die zowel juridisch als praktisch toepasbaar is. Hieronder licht ik toe welke voorbeelden ik heb bestudeerd en waarom juist deze als relevante best practices zijn geselecteerd.

2.5.1 Best practices uit wet- en regelgeving

De belangrijkste voorbeelden zijn afkomstig uit de NIS2-richtlijn, AVG en de NEN7510-norm:

NIS2-richtlijn: Deze richtlijn biedt een uitgebreid kader voor netwerk- en informatiebeveiliging binnen de EU. De keuze voor deze richtlijn was vanzelfsprekend, aangezien het Martini Ziekenhuis onder de nieuwe verplichtingen valt. Specifieke elementen, zoals de vereisten voor tijdige melding (24-72 uur) en de nadruk op het melden van potentiële schade, vormden de basis voor de procedure.

AVG (Algemene Verordening Gegevensbescherming): De AVG biedt duidelijke richtlijnen voor het omgaan met datalekken en meldingen. Dit was cruciaal, gezien de directe impact van deze regelgeving op de bescherming van patiëntgegevens. Vooral het belang van snelle reacties en uitgebreide documentatie van incidenten was een waardevolle input.

NEN7510: Deze norm, specifiek voor informatiebeveiliging in de zorgsector, was een essentieel referentiepunt. De focus op het beschermen van medische gegevens en het uitvoeren van risicoanalyses heeft geholpen om de procedure praktisch toepasbaar te maken binnen de context van een ziekenhuis.

2.5.2 Praktijkvoorbeelden

Naast regelgeving heb ik praktijkvoorbeelden onderzocht van vergelijkbare organisaties en sectoren:

Duitsland en Frankrijk: In deze landen gelden al strengere meldplichtregels, waaronder de melding van bijna- incidenten. Deze praktijkvoorbeelden toonden aan hoe bredere meldplichtcriteria bijdragen aan een vollediger beeld van cyberdreigingen en verhoogde beveiliging.

ITIL Incidentbeheer: Het ITIL-raamwerk (Information Technology Infrastructure Library) bood een gestructureerde aanpak voor incidentmanagement. De focus op categorisatie, prioritering en gestandaardiseerde responsprocessen heeft geholpen bij het ontwikkelen van een praktische en toepasbare procedurebeschrijving.

2.5.3 Verantwoording

De keuze voor deze best practices is gebaseerd op hun directe relevantie voor de context van het Martini Ziekenhuis. De NIS2-richtlijn en AVG vormen de wettelijke basis waar het ziekenhuis aan moet voldoen, terwijl de NEN7510-norm en praktijkvoorbeelden uit het buitenland concrete handvatten bieden voor implementatie. Het ITIL-raamwerk bood daarbij een bewezen methodologie voor incidentbeheer die eenvoudig kan worden geïntegreerd in bestaande processen. Door deze voorbeelden en best practices te bestuderen, was het mogelijk om een procedurebeschrijving te ontwikkelen die voldoet aan de wettelijke eisen en tegelijkertijd praktisch toepasbaar is binnen de complexe omgeving van een ziekenhuis.

2.6 Verwerken definitieve ontwerpeisen in het beroepsproduct

Bij het ontwikkelen van het uiteindelijke beroepsproduct, de procedurebeschrijving voor de meldplicht van cyberincidenten binnen het Martini Ziekenhuis, zijn de definitieve ontwerpeisen uit het theorie- en praktijkonderzoek verwerkt. De keuzes die zijn gemaakt, zijn gebaseerd op een balans tussen wettelijke vereisten, praktische toepasbaarheid en de input van interne betrokkenen. Hieronder wordt beschreven hoe de definitieve ontwerpeisen zijn verwerkt en welke keuzes hieraan ten grondslag liggen.

2.6.1 Verwerking van de definitieve ontwerpeisen

Volledig geïntegreerde eisen

De meeste ontwerpeisen die voortkwamen uit de NIS2-richtlijn, AVG, en NEN7510-norm zijn volledig verwerkt in het beroepsproduct. Dit was noodzakelijk om te voldoen aan de wettelijke verplichtingen en om te zorgen voor een juridisch en technisch kader. Voorbeelden van volledig geïntegreerde ontwerpeisen zijn:

Tijdige meldingsvereisten: De procedure bevat een gestandaardiseerd stappenplan waarin meldingen binnen 24 tot 72 uur moeten worden gedaan, zoals vereist door de NIS2-richtlijn.

Registratie van potentiële schade en bijna- incidenten: Dit sluit aan bij de richtlijnen voor een breder inzicht in het dreigingslandschap, zoals benadrukt door de theorie en de feedback.

2.6.2 Keuzes en afwegingen

Niet alle ontwerpeisen konden volledig worden opgenomen in het beroepsproduct. Dit was deels vanwege verschillen in meningen uit de praktijk en de noodzaak om een hanteerbaar product te creëren. De volgende keuzes zijn gemaakt:

Complexiteit versus toegankelijkheid: Hoewel technische termen en juridische nuances essentieel zijn, is ervoor gekozen om deze te vereenvoudigen in de procedurebeschrijving. Feedbacksessies benadrukten dat eenvoud en toegankelijkheid belangrijker waren voor niet-technisch personeel. Voor verdere (juridische) onderbouwing is dit onderzoek in te zien.

Specifieke scenario's: Hoewel meerdere betrokkenen pleitten voor een uitgebreid aantal scenario's (bijvoorbeeld ransomware versus phishing), is er in het beroepsproduct gekozen geen uitgebreide scenario's op te nemen. Dit was nodig om de procedure overzichtelijk te houden. Mogelijk kan dit in de toekomst worden aangevuld met scenario's in bijlagen.

2.6.3 Divergerende inzichten

Uit het praktijkonderzoek bleek dat sommige betrokkenen, zoals de TSO en CISO, prioriteit gaven aan technische beveiligingseisen, terwijl anderen, zoals de Privacy Officer, meer nadruk legden op juridische compliance.

Na overleg heeft dit geresulteerd in een procedurebeschrijving die enerzijds voldoet aan wettelijke verplichtingen en anderzijds praktisch bruikbaar is voor alle afdelingen.

2.6.4 Conclusie

De definitieve procedurebeschrijving is een vertaling van de ontwerpeisen uit het theorie- en praktijkonderzoek. Door het maken van bewuste keuzes en het afstemmen met de opdrachtgever is een product ontwikkeld dat zowel juridisch onderbouwd als praktisch werkbaar is. Waar mogelijk zijn alle ontwerpeisen verwerkt, en waar concessies nodig waren, is dit afgestemd op de wensen van de betrokkenen en de praktische realiteit van het Martini Ziekenhuis.

2.7 Kwaliteiten en beperkingen

2.7.1 Kwaliteiten en beperkingen

Het onderzoek dat heeft geleid tot de procedurebeschrijving voor de meldplicht van cyberincidenten binnen het Martini Ziekenhuis kent zowel sterke punten als beperkingen. Deze aspecten hebben direct invloed gehad op de kwaliteiten en beperkingen van het uiteindelijke beroepsproduct. In deze paragraaf worden beide in samenhang besproken om een volledig en gebalanceerd beeld te geven van de resultaten.

Kwaliteiten

- **Sterke theoretische basis:** Het onderzoek maakte gebruik van breed erkende regelgeving, zoals de NIS2-richtlijn, AVG en NEN7510. Dit zorgde ervoor dat het beroepsproduct juridisch en technisch goed onderbouwd is. Deze basis helpt het Martini Ziekenhuis bij het voldoen aan wettelijke eisen en versterkt de betrouwbaarheid van het beroepsproduct.
- **Praktijkgerichtheid:** Door middel van interviews en feedbacksessies met betrokkenen werd de aansluiting met de dagelijkse praktijk gegarandeerd. Dit maakte het mogelijk om een procedure te ontwikkelen die niet alleen theoretisch, maar ook praktisch toepasbaar is.
- **Inclusie van verschillende perspectieven:** Het betrekken van juridische, technische en operationele betrokkenen binnen het ziekenhuis heeft gezorgd voor een brede basis van inzichten. Dit resulteerde in een procedure die zowel juridische als organisatorische aspecten integreert.

Beperkingen

- **Beperkte testmogelijkheden:** Omdat de procedurebeschrijving nog niet in real-life is getest, is de praktische toepasbaarheid niet volledig gevalideerd. Dit betekent dat verbeterpunten of knelpunten pas tijdens of na implementatie aan het licht kunnen komen. De belangrijkste consequentie hiervan is dat de effectiviteit en efficiëntie van het beroepsproduct afhankelijk zijn van voortdurende evaluatie en aanpassing.
- **Afwezigheid van kwantitatieve gegevens:** Het onderzoek richt zich sterk op kwalitatieve, zoals interviews en feedbacksessies. Dit maakt het moeilijk om de ontdekkingen te kwantificeren of met cijfers te onderbouwen, wat waardevol zou kunnen zijn bij het tot stand komen van de procedurebeschrijving.
- **Geen externe experts geraadpleegd:** Een belangrijke beperking van het onderzoek is dat er geen externe experts buiten het Martini Ziekenhuis zijn geraadpleegd. Hoewel de interne betrokkenen waardevolle inzichten hebben geboden, kan het ontbreken van input van externe cybersecurity-specialisten of toezichthouders zoals de Autoriteit Persoonsgegevens betekenen dat bepaalde best practices of bredere perspectieven niet volledig zijn meegenomen. Dit kan van invloed zijn op de toepasbaarheid van de procedure. De keuze om geen externe experts te raadplegen, is gemaakt vanwege de verwachting dat de verschillende betrokkenen binnen het Martini Ziekenhuis zelf al diverse werkwijzen, perspectieven en ervaringen zouden aandragen, wat een brede basis zou vormen voor het beroepsproduct. Hierdoor werd besloten om de focus eerst intern te houden en de beschikbare tijd en middelen te richten op het verzamelen van inzichten die specifiek afgestemd zijn op de behoeften van het Martini Ziekenhuis. Hoewel dit een bewuste afweging was, kan het raadplegen van externe experts in een later stadium, bijvoorbeeld bij

de evaluatie van de procedure, alsnog waardevolle aanvullende inzichten opleveren. Vooral op het gebied van grensoverschrijdende regelgeving of complexe cyberdreigingen kan dit een belangrijke bijdrage leveren.

2.7.2 Conclusie

Het onderzoek heeft een waardevol kader opgeleverd dat praktisch ingedeeld is binnen het Martini Ziekenhuis. De procedurebeschrijving biedt een solide basis voor de implementatie van de meldplicht en voldoet aan de wettelijke eisen. Echter, de beperkingen, zoals de afwezigheid van externe experts en de beperkte testmogelijkheden, zorgen dat de procedure mogelijk nog verder verfijning nodig is bij de invoering in de praktijk.

Verbeterpunten voor Toekomstig Onderzoek

Betrekken van externe vergelijkingen:
Toekomstig onderzoek kan uitgebreid worden met casestudies van benchmarkanalyses van andere zorginstellingen die ook werken met de NIS2-richtlijn.

Uitvoeren van een pilotfase:
Een test van de procedure in een afdelingsspecifieke setting zou de bruikbaarheid en effectiviteit ervan verder kunnen valideren.

Combinatie van kwalitatieve en kwantitatieve methoden:
Het gebruik van enquêtes of andere kwantitatieve methoden kan helpen om de bevindingen beter te onderbouwen en een breder draagvlak te creëren.

3. Ontwerpeisen vanuit de theorie

3.1 Inleiding

Dit hoofdstuk geeft antwoord op de theoriedeelvragen zoals genoemd in hoofdstuk 1. Het bespreekt de meldplicht voor cyberincidenten in het kader van de NIS- en NIS2-richtlijnen, met focus op de impact voor het Martini Ziekenhuis. In paragraaf 3.2 wordt ingegaan op de meldplicht en de specifieke ontwerpeisen voor het Martini Ziekenhuis. Paragraaf 3.3 bespreekt de overgang van de NIS-naar de NIS2-richtlijn en de gevolgen voor Europees cyberbeleid. Paragraaf 3.4 behandeld meldingsdrempels en ‘potentiële schade’, inclusief nationale wetgeving en andere kaders zoals de AVG. Tot slot beantwoord paragraaf 3.5. de theoriedeelvragen aan de hand van de in dit hoofdstuk weergegeven theorie uitkomsten.

3.2 Meldplicht voor cyberincidenten

In de context van de aankomende Cyberbeveiligingswet naar aanleiding van de NIS2-richtlijn en de daarbij behorende meldplichten voor cyberincidenten, is het voor het Martini Ziekenhuis van belang om een procedurebeschrijving voor incidentmeldingen in te richten. De NIS2-richtlijn legt de nadruk op het melden van significante incidenten die schade kunnen veroorzaken of daadwerkelijk schade hebben veroorzaakt. Dit betekent dat het ziekenhuis niet alleen incidenten moet melden die directe impact hebben gehad, maar ook die een potentieel risico vormen.

Tijdens de ontwikkeling van de NIS2-richtlijn is gebleken dat er onduidelijkheid bestaat over de exacte criteria voor wat als een meldingswaardig incident moet worden beschouwd. Dit kan uitdagingen opleveren voor de naleving van de wetgeving. Vooral wanneer de definities en meldingsdrempels vaag zijn. Het is daarom belangrijk om in de procedurebeschrijving duidelijke ontwerpeisen op te nemen die rekening houden met deze juridische kaders en de complexiteit van het vaststellen van meldingscriteria. Daarnaast moet de procedurebeschrijving voor de meldplicht van cyberincidenten niet alleen voldoen aan de NIS2-richtlijn, maar ook aan andere relevante wet- en regelgeving rond gegevensbescherming, zoals de AVG en UAVG.

De AVG en UAVG zijn essentieel voor het melden van cyberincidenten omdat ze duidelijke richtlijnen bieden voor het omgaan met datalekken en de bescherming van persoonlijke gegevens. De AVG verplicht organisaties om gegevens te voorkomen tegen verlies, ongeautoriseerde toegang en andere risico's. Bij een datalek dat risico's oplevert voor betrokkenen, moeten organisaties dit binnen 72 uur melden aan de Autoriteit Persoonsgegevens (AP), tenzij er geen risico is.

De meldingsplicht is gericht op het vergroten van schade voor betrokkenen en stelt hen in staat zelf veilige maatregelen te nemen, zoals het wijzigen van wachtwoorden. Daarnaast verplicht de AVG organisaties om technische en ingewikkelde maatregelen te implementeren, zoals monitoring- en meldingsprocessen, om snel op incidenten te reageren. De UAVG, de Nederlandse implementatie van de AVG, past gecorrigeerde nationale richtlijnen toe die specifiek relevant zijn voor het melden van incidenten. Samen zorgen de AVG en UAVG voor duidelijke eisen aan het beheer van datalekken, stimuleren ze betere informatiebeveiliging en ondersteunen ze een tijdige en effectieve reactie op incidenten.[17] Het combineren van deze eisen zorgt voor een volledig beeld van het dreigingslandschap wat waarde toevoegt aan de interne beveiliging en bijdraagt aan de algehele veiligheid van de zorgverlening.[18]

3.3 NIS- Richtlijn

De oorspronkelijke NIS-richtlijn[19] was de eerste Europese wetgeving welke is gericht op het verbeteren van algehele beveiliging van netwerk en informatiesystemen. Een van de belangrijkste elementen van deze richtlijn was de invoering van beveiligingsmaatregelen en meldingsverplichtingen voor essentiële dienstenaanbieders en bepaalde digitale dienstverleners. De richtlijn moest uiterlijk op 9 mei 2018 in nationale wetgeving worden omgezet, en inmiddels hebben alle lidstaten dit gedaan. In Nederland is de NIS-richtlijn geïmplementeerd in de Wet Beveiliging Netwerk- en Informatiesystemen.[20,21]

De richtlijn heeft geholpen om de cyberbeveiliging van landen, bedrijven en overheidsinstanties te versterken en de samenwerking tussen EU-landen te verbeteren. Hierdoor kunnen landen informatie delen en gezamenlijk reageren op dreigingen, terwijl organisaties beter beschermd zijn tegen cyberaanvallen. Door de steeds complexere cyberdreigingen zijn deze maatregelen niet meer voldoende. Daarom is er een nieuwe aanpak nodig, zoals de NIS2-richtlijn, om beter voorbereid te zijn op moderne dreigingen.[22]

Het aantal, de schaal en de impact van cyberincidenten nemen snel toe. Wat een grote bedreiging vormt voor de werking van netwerk- en informatiesystemen. Het Europees Agentschap voor Cyberbeveiliging (ENISA) meldt dat het aantal aanvallen op toeleveringsketens in 2021 vier keer zo hoog was als in 2020, terwijl de oorspronkelijke NIS-richtlijn geen specifieke aandacht besteedde aan de beveiliging van toeleveringsketens.[23] Bovendien zijn aanvallen op cloud-infrastructuren in dezelfde periode zelfs vijf keer toegenomen. Dit laat zien dat cyberdreigingen steeds complexer en diverser worden. Met een groter aantal soorten aanvallen, verschillende doelwitten zoals bedrijven, ziekenhuizen en infrastructuur, en wereldwijde gevolgen die vaak moeilijk te voorspellen zijn, zoals de SolarWinds-hack en ransomware-aanvallen, die zowel grote als kleine organisaties treffen. In Duitsland steeg het aantal ransomware-aanvallen in 2021 met 360%, waarbij een ziekenhuis 13 dagen lang geen nieuwe patiënten kon opnemen na zo'n aanval.[24,25]

Door de toenemende digitalisering in Europa en de toenemende dreigingen op het gebied van cyberbeveiliging werd door de Europese Commissie besloten om de herziening van de richtlijn te versnellen. In december 2020 presenteerde de Commissie daarom een voorstel voor de NIS2-richtlijn. Deze richtlijn heeft als doel om de regels tussen EU-landen beter op elkaar af te stemmen en effectief in te spelen op de expliciete cyberdreigingen.[26] Een belangrijk discussiepunt bij het opstellen van deze wet was welke incidenten precies gemeld moesten worden. De oorspronkelijk NIS-richtlijn verplicht alleen de melding van ernstige incidenten. Wat resulteert in een onvolledig beeld van dreigingen en beperkte mogelijkheden om deze dreigingen te herkennen en erop te reageren. De NIS2-richtlijn streeft naar een betere meldplicht die meer incidenten omvat zodat de EU sneller kan reageren op dreigingen en zich beter kan verdedigen.[27] De NIS 2-richtlijn[28] breidt de meldingsverplichtingen uit en benadrukt het belang van informatie-uitwisseling om de beveiligingsmechanismen te versterken. De verplichte meldplicht blijft een essentieel onderdeel van de NIS 2-richtlijn, maar organisaties kunnen moeite hebben om te bepalen welke incidenten moeten worden gemeld.[29]

Aangezien een onjuiste cybersecurityvoorbereiding en de verspreiding van incidenten grote risico's vormen verplicht de NIS2-richtlijn een verruiming van de meldingsverplichtingen. De richtlijn vereist niet alleen het rapporteren van ernstige incidenten met daadwerkelijke schade, maar ook van incidenten die nog geen schade hebben veroorzaakt maar wel een potentieel risico vormen. Dit maakt de meldingsdremels en de juridische betekenis duidelijk, terwijl ook de cyberweerbaarheid wordt verhoogd.[30,31]

3.3.1 Meldingsverplichtingen: van NIS 1 naar NIS 2

Meldingsverplichtingen zijn niet nieuw binnen de EU-wetgeving. In sectoren zoals telecom en de bank- en financiële sector gelden soortgelijke verplichtingen al langere tijd.[32] Daarnaast is er voor deze sectoren de DORA-wetgeving (Digital Operational Resilience Act). De DORA wetgeving is een Europese verordening. Het doel is om de operationele weerbaarheid van

17 Richtlijn (EU) 2022/9.
18 Brouwer C van Mil 2023, p. 748-757.
19 Richtlijn (EU) 2016/1148.
20 Wbni.
21 'Wbni', wetten.overheid.nl.
22 'Cybersecuritybeeld-nederland', nctv.nl.
23 'ENISA Threat Landscape. 2021', www.enisa.europa.eu.
24 Mittelberg 2020.
25 'IT-Ausfall an der uniklinik Dusseldorf', uniklinik-dusseldorf.de.
26 COM/2020/823.
27 Art 14 Nis- richtlijn.
28 Richtlijn (EU) 2022/2555.
29 'Overzicht van alle onderwerpen/nis2-richtlijn' digitaleoverheid.nl.
30 pbEU 2022, L 333/80.
31 Steenbrugge 2024, p. 302.
32 Gal-Or & Ghose, 2005, p. 186-208.

financiële instellingen te versterken tegen cyberdreigingen en andere IT-gerelateerde risico's. DORA verplicht instellingen in de financiële sector, zoals banken en verzekeraars, om robuuste IT-beveiligingsmaatregelen te implementeren, risico's te monitoren, incidenten te melden en kritieke leveranciers zorgvuldig te beheren.[33]

De NIS-richtlijn heeft een bredere reikwijdte gericht op essentiële onderdelen en bepaalde digitale onderdelen in sectoren die van cruciaal belang zijn voor de interne markt.[34,35] De NIS-richtlijn introduceerde voor essentiële dienstverleners en digitale dienstverleners in sectoren die van cruciaal belang zijn de verplichting om veiligheidsincidenten te melden die een significante impact hebben op de continuïteit van hun dienstverlening. Artikel 14 van de NIS-richtlijn[36] stelt dat essentiële dienstverleners zonder onnodige vertraging incidenten moeten melden die de continuïteit van de essentiële diensten negatief beïnvloeden. Voor digitale dienstverleners in sectoren van cruciaal belang geldt een soortgelijke verplichting, waarbij incidenten met een 'aanzienlijke impact' moeten worden gemeld.[37]

De impact wordt beoordeeld op basis van parameters zoals het aantal getroffen gebruikers, de duur van het incident en de geografische spreiding.[38] De toepassing van deze criteria varieert echter per lidstaat, wat leidt tot inconsistenties bij de interpretatie van wat een 'significant' incident is. Hierdoor kan een incident in het ene land als meldingswaardig worden beschouwd, maar in een ander land niet. De verschillen in interpretatie en toepassing van de meldingsdrempels tussen lidstaten zorgen voor fragmentatie en juridische onzekerheid voor bedrijven. In sommige lidstaten, zoals Duitsland en Frankrijk, gaan de meldingsverplichtingen verder dan de minimumeisen van de NIS-richtlijn en moeten ook potentiële dreigingen of incidenten zonder daadwerkelijke schade worden gemeld.[39,40]

3.3.2 Meldingsverplichtingen onder NIS 2

De NIS2-richtlijn breidt het melden van cyberincidenten verder uit. Onder de richtlijn vallen niet alleen incidenten met daadwerkelijk opgetreden schade, maar ook dreigingen en "bijna-incidenten" die mogelijk ernstig zijn.[41] Door deze situaties te melden, krijgen EU-lidstaten een vollediger beeld van dreigingen, wat hen helpt om beter voorbereid te zijn op toekomstige incidenten. Een ander belangrijk doel van de NIS2-richtlijn is het gelijk trekken van de meldingsverplichtingen tussen de EU- lidstaten. Dit maakt het voor organisaties eenvoudiger om aan de wettelijke eisen te voldoen en hun cyberweerbaarheid te versterken. In de NIS2-richtlijn wordt een incident gedefinieerd als: "gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt."[42] Deze definitie gaat verder dan de oorspronkelijke definitie in de oorspronkelijke NIS-richtlijn, die alleen incidenten omvatte met een daadwerkelijk negatief effect op de veiligheid van netwerk- en informatiesystemen. De NIS2-richtlijn richt zich ook op incidenten die potentieel schade kunnen veroorzaken, zelfs als er nog geen schade heeft plaatsgevonden. Zo wordt de focus niet alleen gelegd op daadwerkelijke impact, maar ook op het potentiële risico van incidenten. Naast de verplichting om incidenten en dreigingen aan de bevoegde autoriteiten te melden, moet een organisatie ook de getroffen dienstontvangers op de hoogte stellen van de dreiging en hen informeren over maatregelen die zij moeten nemen om schade te voorkomen of te beperken.[43]

Veel EU-landen hebben ervoor gekozen om bij de invoering van de oorspronkelijke NIS-richtlijn slechts het minimumniveau van meldingsvereisten op te nemen. Hierdoor is de bestaande meldingsinfrastructuur beïnvloed als een systeem waarin alleen de zwaarste cyberincidenten worden gemeld. Dit betekent dat de meeste nationale systemen alleen rapporteren als er sprake is van grote schade. Hoewel de meldingsvereisten in theorie helder lijken, blijken in de praktijk dat er zwakke gebieden bestaan. Een belangrijk probleem is de juridische beoordeling van incidenten, vooral bij het verschil tussen daadwerkelijke schade (zoals een succesvolle cyberaanval met gegevensverlies) en potentiële schade (zoals een poging tot inbraak in het systeem die wel werd ontdekt maar geen directe schade opleverde). Het onderscheid tussen wat direct schadelijk is en wat een potentieel risico vormt is soms lastig te maken. Dit kan leiden tot onduidelijkheid en twijfel over de verschillen om een incident te melden.[44]

Stel bijvoorbeeld een ziekenhuis ontdekt dat een hacker beperkte toegang heeft tot het patiëntensysteem. Maar de aanval werd tijdig gestopt door beveiligingssoftware. Er is dus geen gevoelige informatie gestolen en er lijkt geen directe schade te zijn. Volgens de traditionele meldingsregels zou dit incident niet gemeld hoeven te worden, omdat er geen enkele schade is ontstaan. Echter, de NIS2-richtlijn zal ook "potentiële schade" laten melden, dus is het ziekenhuis verplicht om dit bijna-incident te rapporteren. Deze verplichtingen kunnen extra werk en kosten met zich meebrengen, en organisaties kunnen ervoor kiezen om sommige incidenten niet te melden vanwege deze onduidelijkheid. Sommige bedrijven maken deze keuze mogelijk uit economisch oogpunt; een melding kan hun reputatie beïnvloeden of leiden tot een onderzoek door toezichthouders. Het is belangrijk om in gedachten te houden dat incidenten met het potentieel om aanzienlijke schade te veroorzaken doorgaans complexer zijn dan bijvoorbeeld een phishing poging, waarvan er dagelijks miljoenen plaatsvinden. Dergelijke pogingen hoeven niet gemeld te worden, tenzij ze succesvol zijn en daarmee de vertrouwelijkheid, integriteit of beschikbaarheid van systemen daadwerkelijk in gevaar brengen. De nieuwe meldingsprocedure van de NIS2-richtlijn volgt een gelaagde aanpak met een vroege initiële waarschuwing binnen 24 uur na het ontdekken van een significant incident, gevolgd door een formele melding binnen 72 uur en, indien nodig, verdere rapportages. Deze vroege melding moet informatie bevatten over de vermoedelijke oorzaak van het incident, bijvoorbeeld

33 DORA.
34 Gordon, Loeb & Lucyshyn 2003, p. 85-461.
35 'Welke sectoren vallen onder de NIS2-richtlijn', nctv.nl.
36 Art 14 Nis- richtlijn.
37 Art 16 Nis- richtlijn.
38 Art 14 Nis-richtlijn.
39 BSI-Wet.
40 pbFr 2009, (decreet nr. 2009-834) t nr 3.
41 Art 23 lid 3 Nis2-richtlijn.
42 Art 6 lid 6 Nis2- richtlijn.
43 Nationaal coördinator terrorismebestrijding en Veiligheid, NIS2-richtlijn, p. 11.
44 Jacobs C Jansen 2024, p. 15-17.

of het mogelijk een onwettige of kwaadaardige daad betreft.[45] De bevoegde autoriteiten of CSIRTs (Computer Security Incident Response Teams) moeten binnen 24 uur reageren op de vroege melding door feedback te geven op het significante incident en eventueel advies te geven over mogelijke maatregelen. De CSIRT kan ook technische ondersteuning bieden als de betrokken entiteit daarom vraagt. Bovendien kunnen extra richtlijnen worden verstrekt als het incident een crimineel karakter heeft.[46]

De melding van een incident moet een update bevatten van de eerder voorziene informatie en een eerste schatting geven van de ernst en gevolgen van het incident. Hierbij moeten, indien mogelijk, indicatoren van compromittering worden opgenomen om aan te geven welke mogelijke elementen getroffen zijn. Indicatoren voor compromittering zijn specifieke tekenen, gegevens van activiteiten die wijzen op een mogelijke cyberaanval of dat er ongeautoriseerde toegang tot een netwerk, systeem of apparaat is uitgevoerd. Deze indicatoren van compromittering helpen beveiligingsteams en -bedrijven om snel een systeem te identificeren dat is gecompromitteerd en wat de aard van de dreiging kan zijn. De CSIRTs zijn bovendien verplicht om informatie door te geven aan andere landen als het incident over de landsgrenzen heen invloed heeft. Zij bepalen ook of het incident publiek moet worden verspreid. Naast hun rol bij de afhandeling van incidenten, moet nationaal hun capaciteit worden uitgebreid om te kunnen aanpassen aan de veranderende dreigingen. Door de toenemende digitalisering en recente politieke ontwikkelingen, zoals de oorlog in Oekraïne, wordt verwacht dat de cyberdreigingen en het aantal meldingen zullen toenemen. Dit vraagt om een grotere inzet en meer middelen om effectief om te gaan met de hoeveelheid aan incidentmeldingen.[47] De uitdaging zit niet alleen in de stijgende dreigingsniveaus, maar ook in het aanzienlijk grotere aantal entiteiten dat onder de NIS2-richtlijn valt. De richtlijn breidt haar toepassing uit naar nieuwe sectoren en hanteert een uniforme drempel voor organisaties die vallen onder de definitie van middelgrote ondernemingen volgens Aanbeveling 2003/361/EG van de Commissie.[48,49]

3.4 Bepalen van de meldingsdrempel: de rol van ‘potentiële schade’

De NIS2-richtlijn biedt geen specifieke richtlijnen voor het bepalen wanneer een incident dat geen schade heeft veroorzaakt toch meldingswaardig is, omdat het incident in staat is ‘ernstige operationele verstoringen of financiële verliezen te veroorzaken’ of ‘andere natuurlijke of rechtspersonen kan treffen door aanzienlijke verliezen te veroorzaken’.[50]

In dit opzicht is het nuttig om te kijken naar de praktijk in lidstaten die al dergelijke uitgebreide meldingsverplichtingen hanteren. Daarnaast kan de verplichte meldingsplicht van datalekken onder de AVG, dienen als voorbeeld dat de meldwaardigheid van een incident of inbreuk kan worden beoordeeld, zelfs als er nog geen schade is opgetreden.

45 Art 23 lid 4 sub a Nis2-richtlijn.
46 Art 23 lid 5 Nis2-richtlijn.
47 Kolby, Morrow & Zbierek, 2022.
48 EG/2003/361.
49 Art 7 jo 9 Nis2-richtlijn.
50 Art 23 lid 3 sub a C b Nis2-richtlijn.

3.4.1 Meldingen in het buitenland

Duitsland en Frankrijk vereisen al de melding van incidenten met potentiële schade in hun nationale wetgeving. In Duitsland moeten bijvoorbeeld incidenten zoals kwetsbaarheden, malware en aanvallen op de IT-beveiliging worden gemeld, zelfs als deze aanvallen succesvol zijn afgeslagen. Dit gebeurt niet voor alledaagse spam, gangbare malware die door standaard antivirusprogramma’s wordt gedetecteerd, of veelvoorkomende technische defecten. De beoordeling of de potentiële schade meldingswaardig is, ligt bij de organisatie, die zich moet afvragen of een melding andere kritische entiteiten kan helpen.[51]

3.4.2 Melding onder de AVG

De AVG vereist dat datalekken worden gemeld tenzij ze waarschijnlijk geen risico vormen.[52] Artikel 4 lid 12 AVG[53] definieert een datalek als een “inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.”[54,55] *Het oplossen van een kwetsbaarheid, bijvoorbeeld* door een patch, is een fundamentele beveiligingsmaatregel. Als een systeem niet tijdig wordt gepatcht, kan dit ook meldingswaardig zijn, zelfs als er geen daadwerkelijke inbreuk is geweest. Het installeren van een patch (Een patch is een software-update die een kwetsbaarheid of fout in een programma oplost om de beveiliging of functionaliteit te verbeteren) wordt gezien als een organisatorische en technische maatregel om een aanval te voorkomen, en wordt volgens Artikel 32 AVG beschouwd als een noodzakelijke technische beveiligingsmaatregel.[56] De richtsnoeren van de EDPB (European Data Protection Board) over meldingsplichtige datalekken maken duidelijk dat een bekende kwetsbaarheid niet gemeld hoeft te worden als er geen toegang tot persoonsgegevens is geweest, omdat dit niet de drempel overschrijdt om een risico voor de betrokkenen te vormen. Wel moet het datalek worden gedocumenteerd in overeenstemming met Artikel 33 lid 5 AVG.[57,58,59]

Het beoordelen van het potentiële optreden van schade en de drempel van significantie zijn cruciaal voor het bepalen of een incident melding plichtig is. Dit ondersteunt het hoofddoel van de NIS2- richtlijn, namelijk het vergroten van cyberweerbaarheid, wat alleen kan worden bereikt als er een volledig beeld is van de huidige dreigingen en trends. De noodzaak om incidenten te melden die geen directe schade hebben veroorzaakt, wordt duidelijker als rekening wordt gehouden met de geavanceerde beveiligingsmechanismen die entiteiten moeten implementeren volgens het NIS-kader. Een handig te gebruiken praktijk, zoals het inzetten van honeypots als beveiligingsmechanisme, kan dit illustreren. Honeypots zijn virtuele vallen om aanvallers aan te trekken; een opzettelijk gecompromitteerd systeem stelt een aanvaller in staat om kwetsbaarheden uit te buiten, zodat de organisatie het gedrag van de aanvaller kan bestuderen en de beveiliging kan verbeteren. Dergelijke lokaalsystemen binnen volledig

51 BSI (Bundesamt für Sicherheit in der Informationstechnik).
52 Art 33 lid 1 AVG.
53 Art 4 lid 12 AVG.
54 Algemene Verordening Gegevensbescherming.
55 Verordening (EU) 2016/679.
56 Art 32 AVG.
57 Art 33 lid 5 AVG.
58 ‘Privacybeleid 2022-2024’, overheid.nl
59 ‘Basis AVG’, autoriteitpersoonsgegevens.nl.

operationele netwerken en servers vormen vaak onderdeel van een inbraakdetectiesysteem. Bij een infiltratie zou een incident in de zin van de NIS2-richtlijn kunnen worden vastgesteld, hoewel het incident alleen potentiële schade veroorzaakt, omdat het zich binnen een gesloten systeem afspeelt.[60]

Een incident dat geen schade heeft veroorzaakt bij de ene entiteit, kan nog steeds een ernstige dreiging vormen voor een andere organisatie. Wanneer de afwezigheid van schade het gevolg is van goede beveiligingsmechanismen, kan het melden van het incident bijdragen aan de evaluatie van het bredere dreigingslandschap en helpen om aanvallen op derden te voorkomen, op te sporen en te verdedigen. Goede detectie- en preventiemaatregelen zijn sterk afhankelijk van regelmatige uitwisseling van informatie over dreigingen en kwetsbaarheden.[61,62]

3.4.3 ITIL melding

De ITIL-standaard (Information Technology Infrastructure Library) is een wereldwijd erkend raamwerk voor IT-servicemanagement dat best practices biedt voor het beheren en optimaliseren van IT- processen. Binnen ITIL speelt incidentbeheer een centrale rol en wordt bedoeld als het proces om verstoringen in de IT-dienstverlening zo snel mogelijk op te lossen of uitgebreid om de normale dienstverlening te herstellen. Bij het melden van incidenten volgens ITIL gaat het om:

2. Het relevante en beïnvloede van verstoringen of storingen in IT-diensten.
3. Het categoriseren en prioriteren van de incidenten.
4. Het geeft aanwijzingen van middelen om effectief op te lossen.

ITIL biedt een gestandaardiseerde aanpak voor incidentbeheer, wat helpt om consistentie en efficiëntie te behalen. Het wordt vaak gezien als een best practice die kan worden toegepast in organisaties om een algemene en bewezen methodiek te gebruiken bij de afhandeling van incidenten. Dit kan eenvoudigweg worden toegepast in bestaande processen, zoals de meldplicht voor cyberincidenten, om snelle respons en minimale verstoring te voorkomen.[63]

3.5 Conclusie

In deze paragraaf wordt aan de hand van de in dit hoofdstuk weergegeven theorie uitkomsten antwoord gegeven op de theoriedeelvragen. Hiertoe wordt in paragraaf 3.5.1. antwoord gegeven op de eerst theoriedeelvraag en in paragraaf 3.5.2. volgt een antwoord op de tweede theoriedeelvraag. De informatie in dit hoofdstuk biedt een antwoord op de deelvragen en impliceert de belangrijkste eisen en implicaties van de NIS2-richtlijn, die relevant zijn voor de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis.

3.5.1 Theoriedeelvraag 1

Ten aanzien van de eerste theoriedeelvraag (*Welke ontwerpeisen voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis zijn relevant in het kader van de aankomende wet- en regelgeving die voortvloeit uit de NIS2-richtlijn omtrent cyberincident meldingen voor het Martini Ziekenhuis?) kan worden geconcludeerd dat de NIS2- richtlijn* een aantal duidelijke eisen stelt aan de meldplichtprocedures. Het Martini Ziekenhuis moet de volgende vereisten in hun procedurebeschrijving opnemen:

Meldplicht voor significante incidenten: Dit omvat incidenten die daadwerkelijke schade of een potentieel risico veroorzaken.

Vroege meldingsprocedure: Een melding moet binnen 24 uur na ontdekking van een incident worden gedaan, gevolgd door een volledige melding binnen 72 uur.

Incidenten zonder directe schade: De procedure moet ook voorzien in de melding van incidenten die geen directe schade hebben veroorzaakt maar een potentieel risico vormen.

Informatie-uitwisseling: Het ziekenhuis moet intern en externe dreigingsinformatie delen, inclusief samenwerking met CSIRTs en andere gezaghebbende autoriteiten.

3.5.2 Theoriedeelvraag 2

Voor de tweede deelvraag (Welke ontwerpeisen voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis kunnen worden afgeleid uit vakliteratuur op het gebied van wettelijke verplichtingen rond de bescherming van persoonsgegevens en regels en procedures die wettelijk zijn vastgelegd voor het melden en afhandelen van cyberincidenten?) blijkt dat de specifieke eisen van de NIS2-richtlijn, andere naast wettelijke verplichtingen zoals de AVG aanvullende vereisten opleggen aan de procedurebeschrijving. De volgende aspecten zijn verkregen van belang:

Meldplicht voor datalekken: De AVG vereist dat datalekken worden gemeld aan toezichthouders als ze een risicovormen voor de rechten en vrijheden van natuurlijke personen.

Documentatie van incidenten: Alle incidenten, meldingsplichtig of niet, moeten gedocumenteerd worden om inzicht te bieden in het dreigingslandschap.

Beoordeling van mogelijke schade: De procedure moet een systematische beoordeling van mogelijke schade bevatten, zelfs bij afwezigheid van daadwerkelijke schade.

Technische maatregelen: Het snel patchen van kwetsbaarheden is essentieel om risico's te beperkt, conform de verplichtingen uit regelgeving en vakliteratuur.

Samenvattend laat dit zien dat de NIS2-richtlijn een uitgebreid en toekomstbestendig raamwerk biedt dat het Martini Ziekenhuis moet toepassen. Door de duidelijk bedoelde meldplicht, een vroege meldingsprocedure, en een verbeterde informatie-uitwisseling te implementeren, kan het ziekenhuis voldoen aan zowel de richtlijn als andere relevante wettelijke verplichtingen, zoals de AVG. Het automatiseren van de meldprocedure en het stimuleren van samenwerking en informatie- uitwisseling zijn essentiële stappen.

60 'Wat is een honeypot' kaspersky.nl.
61 Kranenborg C Verhey 2023, p. 11.
62 Viergever C van Til 2023.
63 Praat 1998, par. 3.6.2.

De nieuwe eisen vermoeden dat meldingen niet langer afhankelijk mogen zijn van de vaststelling van schade. Dit draagt ook bij aan de gezamenlijke preventie en bescherming tegen cyberdreigingen binnen de EU.

4 Ontwerpeisen vanuit de praktijk

4.1 Inleiding

Dit hoofdstuk geeft antwoord op de praktijkdeelvragen zoals genoemd in hoofdstuk 1. Het bouwt voort op de theoretische basis die in hoofdstuk 3 wordt uiteengezet, waarin de meldplicht voor cyberincidenten en de ontwerpeisen vanuit de NIS- en NIS2-richtlijnen worden behandeld. De theorie uit hoofdstuk 3 biedt een kader van verplichte vereisten en richtlijnen die essentieel zijn voor de ontwikkeling van een goed functionerende procedurebeschrijving. Hoofdstuk 4 bespreekt de rol van verschillende betrokkenen binnen het MZH met betrekking tot privacy, informatiebeveiliging en de meldplicht voor cyberincidenten en bouwt voort op de theoretische ontwerpeisen besproken in hoofdstuk 3, met een focus op de implementatie van deze eisen in de praktijk binnen het MZH. De betrokkenen zijn geïnterviewd aan de hand van een vragenlijst, opgenomen als bijlage 2 bij dit onderzoek. Paragraaf 4.2 belicht de Privacy Officer, het toezicht houdt op de AVG- en WGBO-naleving en extra verantwoordelijkheden onder de NIS2-richtlijn. In paragraaf 4.3 wordt de rol van de CISO besproken, inclusief hoe het beveiligingsbeleid wordt ontwikkeld en welke maatregelen bijdragen aan een verbeterde cyberveiligheid. Paragraaf 4.4 behandeld de TSO, die verantwoordelijke is voor de technische IT-beveiliging. De bedrijfsjurist, besproken in paragraaf 4.5, geeft juridisch advies over privacy en regelgeving en werkt samen met de Privacy Officer om patiënten rechten te betwisten. Paragraaf 4.6 bespreekt de Service Manager ICT, die ICT-diensten waarborgt en incidentescalatieprocessen opstelt. Het crisisteam coördineert in paragraaf 4.7 aanvallen zoals cyberincidenten en ontwikkelde toegankelijke protocollen. Paragraaf 4.8 bespreekt de feedback op het concept van de procedurebeschrijving. Tot slot wordt in paragraaf 4.9 aan de hand van de in dit hoofdstuk besproken praktijkuitkomsten antwoord gegeven op de praktijkdeelvragen.

4.2 Privacy Officer

In het kader van de privacybescherming binnen het MZH speelt de Privacy Officer een cruciale rol, met de naam op het gebied van de Wet op de geneeskundige behandelingsovereenkomst (WGBO). ‘De WGBO is een uitgangspunt van hoe we omgaan met patiënten rechten en privacy,’ aldus de Privacy Officer. Deze wet regelt de rechten en plichten van zowel patiënten

als zorgverleners in Nederland en stelt onder andere dat patiënten recht hebben op uitgebreide informatie over hun behandeling, inclusief het recht op inzage in en een kopie van hun medisch dossier. Daarnaast is toestemming van de patiënt vereist voordat een behandeling kan worden uitgevoerd, wat de autonomie van de patiënt versterkt. De WGBO waarborgt ook de privacy van patiënten door zorgverleners te verplichten om te gaan met medische gegevens en duidelijke afspraken te maken over de verantwoordelijkheden in de zorg.

De Privacy Officer moet ervoor zorgen dat de meldplicht voor datalekken, zoals vereist onder de AVG en beschreven in hoofdstuk 3.4.2, volledig wordt geïntegreerd in de procedurebeschrijving. Dit omvat het snel identificeren van risico's en het documenteren van incidenten, ook als deze geen direct risico vormen. Het gaat erom dat we proactief handelen, niet pas als het fout gaat', legt de Privacy Officer uit. Dit houdt in dat er beleid wordt opgesteld, audits worden uitgevoerd en medewerkers worden getraind om bewust te gaan met privacy kwesties. Daarnaast houdt de Privacy Officer toezicht op incidenten, vooral wanneer deze betrekking heeft op persoonsgegevens, en ziet de Privacy Officer toe op de meldplicht bij datalekken. Verder registreert de Privacy Officer risico's en handelt verzoeken van betrokkenen af, zoals inzage- of verwijderingsverzoeken, om zo de rechten van patiënten te betwisten.

Door deze maatregelen draagt de Privacy Officer bij aan het naleven van de WGBO en zorgt ervoor dat de MZH verantwoord omgaat met persoonsgegevens, in lijn met de wettelijke vereisten. Zo wordt niet alleen de privacy van patiënten beschermd, maar wordt ook het vertrouwen in de zorgverlening versterkt.

De nieuwe NIS2-richtlijn stelt hogere eisen aan de beveiliging van netwerken en informatiesystemen. Voor de Privacy Officer betekent dit een uitbreiding van verantwoordelijkheden op het gebied van privacy en gegevensbescherming. De NIS2-richtlijn, zoals beschreven in hoofdstuk 3.3.2, verplicht organisaties om niet alleen significante incidenten met daadwerkelijke schade te melden, maar ook incidenten met een potentieel risico. De Privacy Officer speelt hierin een cruciale rol door te zorgen voor tijdige meldingen aan de bevoegde autoriteiten. Naast de bestaande AVG-verplichtingen moet de Privacy Officer nu ook zorgen voor de NIS2-eisen door het versterken van de cybersecuritymaatregelen binnen de organisatie. Dit omvat risicomanagement, waarbij de Privacy Officer risicoanalyses overdraagt en het beleid ontwikkeld om kwetsbaarheden te vergroten.
Daarnaast is een nauwe samenwerking met IT-teams essentieel voor het evenredig en relevant melden van datalekken en andere incidenten, zoals verplicht onder de nieuwe richtlijn. De strengere toezicht- en sanctiemogelijkheden van NIS2 zorgen voor afwisselend audits en controles. Ook wordt het belang van training en gebruik bij medewerkers verder ingewikkeld om fouten te voorkomen. De Privacy Officer speelt daarmee een cruciale rol bij het respecteren van de NIS2-richtlijn en draagt bij aan de bescherming van persoonsgegevens en de versterking van de beveiliging van het MZH.
Om een cyberincident, zoals een inbreuk op persoonsgegevens, te melden, maakt het MZH gebruik van Zenya. Allereerst wordt ingelogd op het kwaliteitsportaal, Zenya. Binnen dit portaal start een VIN- melding (Veilig Incidenten Melden). Dit type melding is bedoeld voor het rapporteren van incidenten die invloed hebben op patiëntveiligheid, waaronder datalekken of inbreuken op persoonsgegevens. Hier kan worden aangegeven om wat voor incident het gaat, de gegevens die (mogelijk) zijn gelekt en welke systemen betrokken zijn. Uiteindelijk komt deze melding bij de Privacy Officer terecht. De Privacy Officer kijkt vervolgens welke stappen er genomen moeten worden.

4.3 CISO (Chief Information Security Officer)

De Chief Information Security Officer (CISO) is verantwoordelijk voor de implementatie van technische en organisatorische maatregelen zoals vereist door de NIS2-richtlijn en de NEN7510, besproken in hoofdstuk 3.3 en 3.5. Dit omvat het uitvoeren van risicoanalyses en het beheren van kwetsbaarheden, zoals aanbevolen in hoofdstuk 3.4.2. De CISO speelt een strategische rol in het verhogen van de uitgebreide beveiliging en het veronderstellen van volledige informatiebeveiliging bij medewerkers. 'Mijn doel is niet alleen om de systemen veilig te houden, maar ook om ervoor te zorgen dat iedereen binnen het MZH begrijpt waarom informatiebeveiliging zo belangrijk is', legt de CISO uit. De CISO benadrukt dat het MZH voldoet aan de NEN 7510 certificering.

De NEN 7510-norm is de Nederlandse standaard voor informatiebeveiliging in de zorgsector en helpt ziekenhuizen om de privacy en veiligheid van medische gegevens te achterhalen. Deze norm vereist dat ziekenhuizen technische en functionele maatregelen treffen om persoonsgegevens te beschermen tegen ongeautoriseerde toegang, verlies of misbruik. Onder de NEN 7510 moeten risicoanalyses worden uitgevoerd, toegangsbeheer worden ingericht en duidelijke beveiligingsprocedures worden opgesteld. 'We zien de NEN 7510 niet alleen als een inspanning, maar als een manier om het vertrouwen van patiënten te versterken', aldus de CISO. Daarnaast ligt de nadruk op het trainen van medewerkers en het verhogen van bewustzijn rondom informatiebeveiliging. Ook stelt de norm eisen aan incidentenbeheer, waarbij datalekken snel concreet gemeld moeten worden. Door te voldoen aan de NEN 7510 kunnen ziekenhuizen niet alleen aan wettelijke verplichtingen zoals de AVG voldoen, maar ook de veiligheid van patiëntgegevens versterken en vertrouwen opbouwen bij patiënten.

De combinatie van de NEN7510 en de NIS2-richtlijn is van groot belang. Beide hebben als doel om de veiligheid van netwerken en gevoelige informatie te ondermijnen, maar ze richten zich op verschillende aspecten van informatiebeveiliging.

De NEN7510 is een norm die specifiek gericht is op de zorgsector en zich richt op de bescherming van patiëntgegevens en andere therapeutische informatie. De norm benadrukt het voorkomen van datalekken en het conflicteren van de privacy van patiëntgegevens.
De NIS2-richtlijn is een bredere Europese richtlijn die bedoeld is om de netwerk- en informatiebeveiliging in de EU te versterken. De NIS2-richtlijn stelt verplichtingen aan een samenvatting om een nationaal niveau van beveiliging te benadrukken en legt de nadruk op het toenemende risico's voor netwerken en informatie. Organisaties die onder NIS2 vallen, moeten maatregelen nemen om de continuïteit van hun diensten te bestrijden en incidenten te melden die de werking van kritieke infrastructuur kunnen bedreigen. 'De NIS2-richtlijn vraagt ons om vooruit te denken, ook over risico's die misschien nog niet direct zichtbaar zijn,' geeft de CISO aan.

Het belang van de combinatie van NEN7510 en NIS2 ligt in het feit dat ze elkaar aanvullen en organisaties in staat stellen om zowel te voldoen aan nationale als Europese eisen voor

informatiebeveiliging. Door beide normen te combineren, kunnen organisaties niet alleen hun informatiesystemen beter beschermen, maar ook sneller reageren op dreigingen en incidenten, wat essentieel is voor het behoud van de continuïteit van hun diensten.

Tot slot draagt de combinatie van NEN7510 en de NIS2-richtlijn bij aan een toekomstbestendige aanpak van informatiebeveiliging. De NIS2-richtlijn verzwaart de samenwerking tussen Europese lidstaten gezamenlijke met het aanpakken van grootschalige incidenten, terwijl NEN7510 zorgt voor gedetailleerde beveiligingsmaatregelen die specifiek zijn afgestemd op de zorgsector. We bereiden ons voor op een steeds complexere wereld, waarin cybersecurity geen bijzaak meer is, maar een kernwaarde van onze organisatie,' besluit de CISO. Door beide normen te beheersen, kan het MZH haar beveiligingspraktijken vormgeven en zich voorbereiden op de steeds complexere uitdagingen op het gebied van cybersecurity.

4.4 TSO (Technische Security Officer)

De Technisch Security Officer zorgt ervoor dat de IT-infrastructuur en systemen van het MZH optimaal beveiligd zijn tegen cyberdreigingen. Het is mijn taak om potentiële zwakheden voor te zijn en ervoor te zorgen dat onze systemen continu beschermd zijn,' legt de TSO uit. Dit begint met het bijhouden van potentiële componenten in systemen, netwerken en applicaties door middel van risicoanalyses en penetratietests. Op basis van deze testen en analyses werkt de TSO samen met andere IT-teams om beveiligingsmaatregelen te implementeren, zoals firewalls, inbraakdetectie/preventiesystemen en encryptie.

Daarnaast houdt de TSO zich bezig met het opstellen en onderhouden van beveiligingsbeleid en procedures die de technische veiligheid met zich meebrengen. 'Het beleid is niet alleen een papieren werkelijkheid; het vormt de basis voor hoe we werken en reageren,' aldus de TSO. Ze monitoren voortdurend de systemen op verdachte activiteiten en reageren adequaat op beveiligingsincidenten door forensisch onderzoek uit te voeren en herstelacties te veroorzaken. Dit omvat de samenhangende oorzaak van het incident en het ontwikkelen van preventieve maatregelen om herhaling te voorkomen. De TSO speelt een belangrijke rol bij het beoordelen of een incident voldoet aan de meldcriteria zoals gedefinieerd in hoofdstuk 3.4. Dit omvat zowel incidenten met daadwerkelijke schade als potentiële risico's die een dreiging vormen voor de continuïteit van IT- systemen.

Een belangrijk aspect van het werk is ook het up-to-date houden van de technische kennis over de laatste cyberdreigingen en beveiligingstechnologieën. De TSO stimuleert de organisatie over nieuwe trends en ontwikkelingen en zorgt ervoor dat alle systemen voldoen aan wettelijke en branche gerelateerde compliance-eisen, zoals GDPR, ISO 27001 of NIST-normen. 'Deze standaarden helpen ons niet alleen om risico's te minimaliseren, maar ook om vertrouwen te creëren bij patiënten en stakeholders,' legt de TSO uit.

GDPR, ISO 27001 en NIST-normen zijn belangrijke kaders en standaarden die het MZH helpen bij het waarborgen van gegevensbescherming en informatiebeveiliging. De General Data Protection Regulation (GDPR) is een Europese privacywet die voorschrijft hoe organisaties persoonsgegevens moeten verzamelen, opslaan en verwerken. Het doel is om de privacyrechten van individuen te beschermen, waarbij strenge eisen worden gesteld aan transparantie, dataminimalisatie en beveiliging. Overtredingen kunnen leiden tot hoge boetes. ISO 27001 is een internationale standaard voor informatiebeveiligingsmanagement. Het biedt een gestructureerde aanpak voor het implementeren, onderhouden en continu verbeteren van een Information Security Management System (ISMS). Door te voldoen aan ISO 27001 kan het MZH aantonen dat ze systematisch omgaan met informatiebeveiligingsrisico's, zoals datalekken of cyberaanvallen.

De NIST-normen, ontwikkeld door het National Institute of Standards and Technology in de VS, vormen een reeks richtlijnen en best practices voor cybersecurity. Een van de meest gebruikte frameworks, het NIST Cybersecurity Framework (CSF), helpt organisaties bij het identificeren, beschermen tegen, detecteren, reageren op en herstellen van cyberdreigingen. Samen bieden deze kaders voor het MZH een basis voor het beschermen van gevoelige informatie en het naleven van wettelijke en branche gerelateerde eisen.

De TSO geeft aan belang te hebben bij de procedurebeschrijving van de meldplicht. En beveelt aan om bijna incidenten mee te nemen in de beschrijving. Er komen namelijk wel "near miss" situaties voor waarbij bijvoorbeeld: een ransomware-aanval tijdig wordt gestopt door de firewall (beveiligingsmaatregel van het MZH). 'Zelfs als een ransomware-aanval wordt gestopt door een firewall, moeten we dat registreren en analyseren,' benadrukt de TSO. Hoewel er geen gegevensverlies heeft plaatsgevonden, zou dit incident volgens de NIS2-richtlijn als een bijna-incident moeten worden gemeld. De TSO pleit voor het opnemen van duidelijke richtlijnen voor deze situaties in de procedurebeschrijving van de meldplicht. Daarnaast is het van belang om duidelijke communicatiestromen op te nemen in de procedure, er wordt namelijk gebruik gemaakt van SENO, dit is een communicatieplatform waar het security responseteam gebruik van maakt, maar ook wordt er gecommuniceerd via Teams en face to face. 'Een snelle en duidelijke communicatie kan het verschil maken bij het oplossen van een incident,' aldus de TSO.

4.5 Bedrijfsjurist

Een bedrijfsjurist binnen het MZH adviseert over juridische vraagstukken, zoals contracten, privacy (bijvoorbeeld naleving van de AVG), arbeidsrecht, en aansprakelijkheid. 'Onze rol is ervoor te zorgen dat het ziekenhuis juridisch veilig opereert, zonder dat het proces van zorgverlening in het gedrang komt,' vertelt de bedrijfsjurist. Zo ondersteunen ze het MZH bij het beperken van juridische risico's en waarborgen ze een juridisch veilige bedrijfsvoering.

Met name het beroepsgeheim en het belang van pseudonimiseren van gegevens wordt aan de aandacht gebracht wanneer de bedrijfsjurist wordt gevraagd naar privacybeveiliging. 'Het pseudonimiseren van gegevens is niet alleen een technische kwestie, maar ook een juridisch fundament voor privacybescherming.' Hierover wordt regelmatig overleg gepleegd tussen de bedrijfsjurist en Privacy Officer. Hoewel beroepsgeheim en pseudonimisering geen directe rol spelen in de meldplicht van cyberincidenten, is de juridische basis, zoals vastgelegd in de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO), relevant voor de algemene gegevensbescherming binnen het MZH.

De WGBO regelt de rechten en plichten van patiënten en zorgverleners in Nederland. ‘Deze wet is erop gericht om een gelijkwaardige en transparante relatie tussen patiënt en gezondheidszorg te delen,’ aldus de bedrijfsjurist. Deze wet verplicht zorgverleners om patiënten goed te informeren over hun behandeling, zodat zij een weloverwogen beslissing kunnen nemen. Ook legt de WGBO vast dat patiënten recht hebben op inzage in hun medisch dossier en dat zorgverleners medische gegevens vertrouwelijk moeten behandelen. ‘Het is ons doel om te zorgen dat patiënten zich gehoord en beschermd voelen’, zegt de bedrijfsjurist.

Daarnaast mogen behandelingen alleen worden uitgevoerd met toestemming van de patiënt, tenzij er sprake is van een noodsituatie. De WGBO waarborgt daarmee een gelijkwaardige en transparante relatie tussen patiënt en zorgverlener. ‘Dit lijkt soms een grijs gebied, maar duidelijke juridische kaders helpen ons bij het nemen van consistente besluiten,’ legt de bedrijfsjurist uit.

Dit aspect is ook van belang bij de bredere context van privacybescherming en de meldplicht, vooral wanneer persoonsgegevens betrokken zijn. Zo kan de bedrijfsjurist juridisch advies geven over de beoordeling van potentiële schade, zoals beschreven in hoofdstuk 3.4, en erop toezien dat de interpretatie van meldingscriteria consistent blijft met de NIS2-richtlijn en nationale wetgeving. ‘In essentie is mijn werk een balans vinden tussen juridische onjuist en praktische verdeeldheid,’ besluit de bedrijfsjurist. Zo speelt de bedrijfsjurist een rol in het behalen van een juridisch veilige bedrijfsvoering binnen het MZH.

4.6 Service Manager ICT

De Service Manager ICT binnen het MZH is verantwoordelijk voor het waarborgen van de continuïteit en kwaliteit van de ICT-diensten. ‘Mijn voornaamste doel is ervoor te zorgen dat de technologie naadloos aansluit op de behoeften van zorgprofessionals en verdeelde afdelingen,’ legt de Service Manager uit. Dit omvat het coördineren van incidentbeheer, het optimaliseren van serviceprocessen en het bewaken van de naleving van Service Level Agreements. Daarnaast monitoren ze de prestaties van ICT-systemen, stellen ze verbeterplannen op en dragen ze zorg voor tijdige updates en onderhoud. Het ultieme doel is het creëren van een stabiele en efficiënte ICT-omgeving, zodat de medische processen zonder onderbrekingen kunnen verlopen. ‘Het draait om stabiliteit en betrouwbaarheid als ICT faalt, kan dat directe gevolgen hebben voor de zorg aan patiënten,’ is wat de Service Manager ICT aangeeft.

Een belangrijk onderdeel van de functie is het beheren van klachten en escalaties. De Helpdesk fungeert als eerste aanspreekpunt voor klachten, maar wanneer deze niet kunnen worden opgelost, worden ze overgedragen naar de Service Manager. ‘Soms gaat het niet alleen om een technische oplossing, maar ook om het creëren van vertrouwen bij de gebruiker’, vertelt de Service Manager. Klachten die te maken hebben met privacygevoelige kwesties worden direct doorgezet naar de Privacy Officer. Bijvoorbeeld: als er een incident wordt gemeld via de helpdesk dat mogelijk verband houdt met een phishingaanval, moet de Service Manager dit direct escaleren naar de Privacy Officer of het crisisteam, afhankelijk van de aard van het incident. ‘We kunnen het ons niet permitteren om fouten te maken bij dit soort kwesties,’ de Service Manager doel toe.

Om incidenten effectief te kunnen afhandelen, heeft de Service Manager aangegeven baat te hebben bij een duidelijk stappenplan. ‘Het zou enorm helpen om een gedetailleerd protocol te hebben met concrete voorbeelden en scenario’s,’ begrijpelijk de Service Manager. Het stappenplan moet voldoen aan de eisen uit hoofdstuk 3.5, zoals de vroege meldingsprocedure (binnen 24 uur) en de volledige melding (binnen 72 uur). Het beschrijft onder andere hoe snel een melding moet worden gedaan, bij wie deze moet worden ingediend en welke vervolgstappen genomen moeten worden. ‘Zo’n handvat geeft niet alleen structuur, maar zorgt er ook voor dat iedereen op dezelfde manier handelt, bepaalde situatie,’ stelt de Service Manager. Door deze aanpak kan de ICT-afdeling consistent en doelgericht te werk gaan, waardoor de risico’s voor de organisatie beperkt worden en de zorgprocessen soepel blijven verlopen.

4.7 Crisisbeheersing

Het crisisteam binnen het MZH is verantwoordelijk voor het coördineren en aanpakken van noodsituaties binnen het MZH. ‘In een crisis is snelheid belangrijk, maar zonder structuur loopt het al snel mis,’ legt een lid van het crisisteam uit. Hun taken omvatten het inschatten van de situatie, het nemen van snelle beslissingen en het inzetten van beschikbare middelen om de crisis onder controle te krijgen. Ze zorgen ervoor dat protocollen worden gevolgd, communiceren met betrokken partijen (zoals personeel en externe hulpdiensten), en nemen maatregelen om de impact op patiënten, medewerkers en systemen te minimaliseren. ‘Onze prioriteit is om de schade te voorkomen en het ziekenhuis operationeel te houden,’ aldus de crisisadviseur. Daarnaast werkt het crisisteam aan het ontwikkelen van scenario’s en plannen om voorbereid te zijn op mogelijke toekomstige crisissituaties. Binnen de crisisbeheersing zijn er medewerkers die 24/7 beschikbaar zijn, waaronder ICT-specialisten, bedrijfshulpverleners (BHV’ers), clustermanagers en een chirurg. ‘Het is belangrijk dat we op elk moment een multidisciplinair team paraat hebben,’ legt de crisisadviseur uit. Voor het omgaan met crisissituaties zijn er twee noodplannen opgesteld. Het eerste plan richt zich op situaties waarbij er een probleem is met de voorzieningen. In dergelijke gevallen wordt het noodplan gevolgd door de dienstdoende medewerkers die op dat moment aanwezig/bereikbaar zijn. Het tweede, patiëntgerichte noodplan is specifiek bedoeld voor situaties waarbij patiënten direct betrokken zijn, zoals bij kwetsbare patiënten of de handmatige van opvang. ‘Voor dit soort vertrouwenssituaties kiezen we vaak voor de expertise van de dienstdoende chirurg’, aldus de crisisadviseur.

Momenteel werkt crisisbeheersing aan het ontwikkelen van scenario’s om meer gestructureerde en heldere stappen te creëren voor verschillende soorten situaties. ‘We hebben opgemerkt dat duidelijke scenario’s enorm helpen om in stressvolle situaties beslissingen te nemen,’ zegt de crisisadviseur. Een procedurebeschrijving betreft cyberincidenten sluit hier dan ook goed bij aan. De crisisadviseur geeft aan dat het nuttig is om in een dergelijk scenario of beschrijving de volgende punten op te nemen:

- Het tijdsbestek waarin gehandeld moet worden.
- Wie geïnformeerd moeten worden over het incident.
- Wanneer er wel of niet actie moet worden ondernomen.
- Welke systemen betrokken zijn.
- Hoe gehandeld moet worden als een specifiek systeem wordt geraakt.
- Wat de mogelijkheden zijn om een getroffen systeem door een ander systeem te laten vervangen.

De scenario's voor crisisbeheersing moeten rekening houden met de meldingsvereisten zoals beschreven in hoofdstuk 3.4, inclusief meldingen van incidenten zonder directe schade maar met potentiële risico's. Een voorbeeld hiervan is een poging tot inbraak in het systeem die tijdig is gestopt, maar waarbij de impact op patiëntgegevens onduidelijk blijft.

Daarnaast is er de vraag of het zinvol is om een vooraf bepaald bedrag voor losgeld vast te stellen. Zoals aanbevolen in hoofdstuk 3.4.3, moet het beleid omtrent losgeld duidelijk worden vastgelegd, inclusief de maximale bedragen en beslissingsbevoegdheden bij ransomware-incidenten. *Hiermee weten betrokken medewerkers* of zij in een situatie waarin losgeld wordt geëist, wel of niet mogen betalen en tot welk bedrag. Tevens moet worden vastgelegd wie in deze situaties de bevoegdheid heeft om te handelen. 'In de chaos van een ransomware-incident helpt het als iedereen precies weet wie verantwoordelijk is', aldus de crisisadviseur.

Een belangrijk aandachtspunt voor het crisisteam is dat de opgestelde stappen niet alleen duidelijk zijn, maar ook begrijpelijk vertaald worden naar de rest van het ziekenhuis. Het heeft geen zin om een perfect plan te hebben als niemand het begrijpt,' stelt de crisisadviseur. 'Daarom werken we aan communicatieve vertalingen van onze protocollen, zodat alle medewerkers weten wat ze moeten doen in het geval van een incident.' Het crisisteam blijft zo werken aan een veiliger en beter voorbereid ziekenhuis.

4.8 Feedback

4.8.1 Procedure voor Cyberincidentmelding Martini Ziekenhuis – Overzicht van Aanpassingen

Naar aanleiding van de feedbacksessies zijn er aanpassingen doorgevoerd in het concept van de procedurebeschrijving. De feedbacksessies hebben geresulteerd in aanpassingen die de procedurebeschrijving sterker laten aansluiten op de eisen uit de NIS2-richtlijn en AVG, zoals beschreven in hoofdstuk 3. Dit omvat verbeteringen in de definities, meldingscriteria en communicatieprocessen. Over het geheel van de procedurebeschrijving is naar aanleiding van de feedback een controle gedaan op gebruik van overbodige woorden, dit is gedaan om de gegeven informatie zo duidelijk mogelijk te maken. En er is een controle gedaan op het gebruik van hoofdletters, sommige afkortingen en termen behoren namelijk wel of niet in hoofdletters te zijn weergegeven.

De volgende specifieke aanpassingen zijn na de feedback uitgevoerd:

Doel en Toepassingsgebied
Ontvangen feedback: Het doel van de procedure was te breed omschreven en niet direct gekoppeld aan de wettelijke vereisten.
Actie ondernomen: De beschrijving van het doel is aangescherpt om te benadrukken dat de procedure gericht is op het voldoen aan de NIS2-richtlijn, NEN7510 en AVG. **Verantwoording:** Dit benadrukt het belang van tijdige en accurate meldingen voor wettelijke naleving en operationele veiligheid.

Definities
Ontvangen feedback: Er werd aangegeven dat termen zoals "Significant Incident" en "NIS2-Richtlijn" onvoldoende duidelijk waren.
Actie ondernomen: Meer specifieke definities zijn toegevoegd, inclusief concrete voorbeelden van wat een significant incident inhoudt.
Verantwoording: Dit verduidelijkt welke incidenten gemeld moeten worden en legt de nadruk op potentiële risico's, zelfs bij dreigingen zonder directe schade.

Begrijpelijkheid voor Niet-Technisch Personeel
Ontvangen feedback: Tijdens een feedbacksessie werd aangegeven dat bepaalde technische termen (zoals "penetratietest" en "risicoanalyse") niet duidelijk waren.
Actie ondernomen: Technische termen zijn toegelicht in een definitie lijst aan het begin van de procedurebeschrijving.
Verantwoording: Dit maakt de procedure begrijpelijker voor niet-technisch personeel, waardoor de implementatie soepeler verloopt.

Aandacht voor Bijna-Incidenten ("Near Misses")
Ontvangen feedback: De feedback vraagt om expliciete aandacht voor bijna-incidenten, omdat deze een waardevol inzicht bieden in potentiële risico's.
Actie ondernomen: Een sectie in de procedure beschrijft hoe bijna-incidenten moeten worden gerapporteerd, geanalyseerd en meegenomen in risicomanagement.
Verantwoording: Dit sluit aan bij de NIS2-richtlijn en versterkt de interne cyberweerbaarheid van het Martini Ziekenhuis.

Verplichte Meldingscriteria
Ontvangen feedback: De criteria voor verplichte meldingen waren niet specifiek genoeg.
Actie ondernomen: De formulering is aangescherpt om expliciet te maken dat incidenten met significante impact onmiddellijk gemeld moeten worden.
Verantwoording: Dit garandeert naleving van de NIS2-vereisten en minimaliseert vertraging in meldingsprocessen.

Criteria voor Significante Incidenten
Ontvangen feedback: Er was behoefte aan voorbeelden om de toepasbaarheid te verduidelijken.
Actie ondernomen: Voorbeelden zoals systeemuitval of problemen met gegevensintegriteit zijn toegevoegd.
Verantwoording: Dit maakt het eenvoudiger voor gebruikers om incidenten correct te classificeren.

Definitie van "Significant Incident"
Ontvangen feedback: De CISO merkt op dat de definitie van "significant incident" in het concept te abstract is en kan leiden tot interpretatieverschillen.
Actie ondernomen: Een gedetailleerdere definitie met concrete voorbeelden is toegevoegd, zoals: Incidenten waarbij meer dan 100 patiëntendossiers zijn betrokken.
Uitval van IT-systemen die directe invloed hebben op patiëntenzorg.

Verantwoording: Dit maakt de procedure duidelijker en voorkomt misverstanden bij technisch en niet-technisch personeel.

Coördinatie met Autoriteiten
Ontvangen feedback: De communicatie met nationale cybersecurityautoriteiten bij grensoverschrijdende incidenten moest beter worden belicht.
Actie ondernomen: Er is meer nadruk gelegd op het belang van deze communicatie.
Verantwoording: Dit versterkt de samenwerking en naleving van wettelijke verplichtingen.

Melding aan Autoriteit Persoonsgegevens
Ontvangen feedback: Geen specifieke feedback ontvangen.
Actie ondernomen: De beschrijving is aangescherpt met verwijzingen naar Artikel 33 van de AVG.
Verantwoording: Dit versterkt de juridische nauwkeurigheid van de procedure.

Patching en Mitigatiemaatregelen
Ontvangen feedback: Het belang van snelle actie bij kwetsbaarheden werd benadrukt.
Actie ondernomen: De verplichting om kwetsbaarheden snel te patchen is expliciet toegevoegd.
Verantwoording: Dit versterkt de beveiliging en vermindert het risico op niet-naleving.

Communicatie met Betrokkenen
Ontvangen feedback: Er was behoefte aan meer gedetailleerde communicatie-eisen voor getroffen patiënten.
Actie ondernomen: Naast informatie over de aard van de dreiging zijn aanbevolen acties en ziekenhuismaatregelen toegevoegd.
Verantwoording: Dit bevordert vertrouwen en duidelijkheid bij patiënten.

Verbetering van Communicatie over Rollen en Verantwoordelijkheden
Ontvangen feedback: De feedback benadrukte dat verantwoordelijkheden tussen teams niet altijd duidelijk waren in het conceptdocument.
Actie ondernomen: Een overzicht van verantwoordelijkheden is toegevoegd, waarin wordt gespecificeerd wie, wat, wanneer moet doen tijdens een incidentmelding.
Verantwoording: Dit zorgt voor duidelijkheid en voorkomt dubbel werk of verwarring tijdens incidenten.

Tot slot is er naar aanleiding van de feedback een afspraak gemaakt dat de procedurebeschrijving na aanpassing van de feedback wordt weergegeven in de Martini-Layout zodat deze kan worden opgenomen in het kwaliteitsportaal van het MZH, wanneer de procedurebeschrijving is gepubliceerd in het kwaliteitsportaal zal deze zichtbaar en bruikbaar zijn voor alle medewerkers van het MZH.

4.9 Conclusie

In deze paragraaf wordt aan de hand van de in dit hoofdstuk weergegeven praktijkervaringen en de feedbacksessies antwoord gegeven op de deelvragen. Hiertoe wordt in 4.9.1 antwoord gegeven op de eerste praktijkdeelvraag en in 4.9.2. wordt antwoord gegeven op de tweede praktijkdeelvraag. Praktijkervaringen en de feedbacksessies hebben aangetoond dat er een duidelijke noodzaak is voor een sterke koppeling tussen de theoretische meldplicht, zoals uitgewerkt in hoofdstuk 3.5, en de implementatie daarvan in de dagelijkse praktijk. Deze implementatie, zoals vastgelegd in hoofdstuk 4.8, onderstreept het belang van praktische toepasbaarheid en concrete procedures.

4.9.1 Praktijkdeelvraag 1

Ten aanzien van de eerste praktijkdeelvraag (Welke ontwerpeisen voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis zijn af te leiden uit de kennis en ervaring van interne betrokkenen, relevant t.a.v. het onderwerp, op het gebied van cyberveiligheid en de implementatie van de verplichtingen voortvloeiend uit de NIS2-richtlijn voor het Martini Ziekenhuis?) kan op basis van de verstrekte informatie de volgende ontwerpeisen voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis worden afgeleid:

Duidelijke verantwoordelijkheden: Specificeer de rol van de Privacy Officer, CISO, TSO, en andere betrokkenen, inclusief wie verantwoordelijk is voor het melden en coördineren van acties. Zorg voor een expliciete toewijzing van bevoegdheden bij beslissingen, zoals het betalen van losgeld of het escaleren van incidenten.

Heldere stappenplannen: Ontwikkel een concreet stappenplan met richtlijnen voor het melden en afhandelen van cyberincidenten, zoals:
- Tijdslimieten voor het melden van incidenten.
- Specificeren wie geïnformeerd moet worden (intern en extern).
- Beschrijven van acties bij verschillende typen incidenten.

Scenario's en training: Ontwerp scenario's voor veelvoorkomende incidenten, inclusief "bijna-incident" situaties, om te oefenen en medewerkers voor te bereiden op snelle en effectieve reacties. Verwerk deze scenario's in regelmatige trainingen en simulaties.

Integratie van NIS2 en NEN7510: Zorg ervoor dat de procedure voldoet aan de eisen van de NIS2- richtlijn (zoals risicomanagement en continuïteit van kritieke systemen) en de NEN7510-standaard (voor bescherming van medische gegevens).
Combineer de focus op privacy (AVG, WGBO) met technische beveiligingseisen (ISO 27001, NIST).

Technische details: Definieer welke systemen betrokken zijn en hoe herstel of vervanging moet plaatsvinden als een systeem geraakt wordt.
Beschrijf het gebruik van beveiligingstechnologieën zoals encryptie, firewalls, en inbraakdetectie.

Communicatie: Beschrijf wie wanneer moet communiceren en met welke inhoud.

Toegankelijkheid en eenvoud: Zorg dat de procedure begrijpelijk is voor alle betrokkenen, ook buiten de ICT afdeling en het crisisteam, om het hele ziekenhuis effectief in staat te stellen te reageren. Vertaal complexe technische of juridische begrippen naar begrijpelijke taal.

Controle en verbetering: Implementeer periodieke audits en evaluaties van de procedure om de effectiviteit te controleren en bij te sturen waar nodig. Documenteer incidenten en bijna-incidenten om te leren van ervaringen.

4.9.2 Praktijkdeelvraag 2

Voor de tweede praktijk deelvraag (Welke ontwerpeisen voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis zijn af te leiden uit een feedbacksessie van het concept procedurebeschrijving met het personeel, IT-experts en management van het ziekenhuis?) kunnen op basis van een feedbacksessie de volgende ontwerpeisen worden afgeleid voor de procedurebeschrijving omtrent de meldplicht voor cyberincidenten:

Duidelijkheid en toegankelijkheid van de procedure: De procedure moet begrijpelijk zijn voor alle betrokkenen, inclusief niet-technisch personeel. Het taalgebruik moet eenvoudig zijn en jargon moet worden uitgelegd in een sectie met definities. Tekstgebruik is kort en duidelijk zonder overbodige woorden.

Specifieke meldingscriteria: Er moeten duidelijke criteria zijn voor het bepalen welke incidenten significant genoeg zijn om te melden. Dit omvat een definitie van “significant incident”. Maar ook een verduidelijking van wanneer iets wel of geen cyberincident is.

Vroege waarschuwing en follow-up: Een proces voor een vroege waarschuwing van interne en externe belanghebbenden moet worden opgenomen, evenals een gestructureerde evaluatie van incidenten na afloop.

Technische en juridische conformiteit: De procedure moet voldoen aan relevante wet- en regelgeving (zoals NIS2, NEN7510, AVG) en technische standaarden, inclusief richtlijnen voor patching en het documenteren van datalekken.

Betrokkenheid van stakeholders: De procedure moet ruimte laten voor input en samenwerking van verschillende stakeholders, inclusief management en technische teams, om ervoor te zorgen dat deze breed gedragen wordt.

Training en bewustwording: De procedure moet gepaard gaan met een verplichting voor regelmatige training en bewustwording, zodat personeel adequaat kan reageren op cyberincidenten.
Deze ontwerpeisen zorgen ervoor dat de procedure niet alleen voldoet aan wettelijke vereisten, maar ook praktisch uitvoerbaar is en aansluit bij de dagelijkse operationele realiteit van het ziekenhuis.

Samenvattend laat dit zien dat de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis een cruciale rol speelt in het waarborgen van zowel technische als juridische conformiteit. Door een combinatie van duidelijke verantwoordelijkheden, toegankelijke procedures en een sterke integratie van NIS2-, NEN7510- en AVG-vereisten kan het ziekenhuis voldoen aan de richtlijnen en tegelijkertijd een veilige en betrouwbare omgeving creëren.
Het ontwikkelen van heldere stappenplannen, het automatiseren van meldprocessen en het bevorderen van training en samenwerking dragen bij aan de praktische uitvoerbaarheid. De nadruk op het melden van bijna-incidenten en een proactieve aanpak van risicomanagement versterken de preventie en bescherming tegen cyberdreigingen. Het ziekenhuis kan zo niet alleen beter reageren op incidenten, maar ook bijdragen aan een bredere informatie-uitwisseling en samenwerking binnen de sector, wat de algehele cybersecurity van het MZH versterkt. De ontwerpeisen zullen worden meegenomen in ontwikkeling van de procedurebeschrijving (bijlage 1).

5. Analyse en conclusie

5.1 Inleiding

Dit hoofdstuk analyseert de ontwerpeisen voor de procedurebeschrijving op basis van het voorgaande onderzoek. Het bouwt voort op de theoretische basis die in hoofdstuk 3 is uiteengezet, waarin de meldplicht voor cyberincidenten en de ontwerpeisen vanuit de NIS2-richtlijn en AVG centraal staan. Deze theoretische basis biedt een kader van verplichte vereisten en richtlijnen die essentieel zijn voor de ontwikkeling van een goed functionerende procedurebeschrijving. Daarnaast sluit dit hoofdstuk aan op de praktijkinzichten die in hoofdstuk 4 zijn besproken, waarin de rol van betrokkenen en feedbacksessies binnen het Martini Ziekenhuis centraal staan. In paragraaf 5.2 wordt in 5.2.1. weergegeven wat de overeenkomsten tussen theorie en praktijk zijn. Vervolgens komen in paragraaf 5.2.2. de conflicten tussen theorie en praktijk aan bod. Gevolgd door in 5.2.3. de keuzes en prioritering. De conclusies in paragraaf 5.3 formuleren definitieve ontwerpeisen voor de meldplichtprocedure, gebaseerd op een analyse van theorie, praktijkervaringen en feedback. Dit hoofdstuk biedt daarmee de benodigde inzichten en aanbevelingen voor een effectieve en praktisch uitvoerbare meldplichtprocedure binnen het Martini Ziekenhuis.

5.2 Analyse van de Ontwerpeisen

5.2.1 Overeenkomsten tussen theorie en praktijk

Het onderzoek heeft aangetoond dat er grote overeenkomsten zijn tussen de theoretische ontwerpeisen, weergegeven in hoofdstuk 3 (zoals de wettelijke verplichtingen uit de NIS2-richtlijn, AVG en NEN7510) en de praktische behoeften, weergegeven in hoofdstuk 4, van het Martini Ziekenhuis:

Helderheid en eenvoud: Zowel vanuit de regelgeving als de feedback en interviews van betrokkenen werd benadrukt dat een duidelijke en eenvoudige procedure essentieel is. Dit is verwerkt door het gebruik van een gestandaardiseerd stappenplan en toegankelijke taal.
Tijdige meldingen: De wettelijke vereisten rondom het melden van incidenten binnen 72 uur werden volledig onderschreven door de praktijkinzichten. Dit benadrukt het belang van snelheid bij incidentmanagement zoals ook aan bod is gekomen tijdens de interviews.

Bijna-incidenten: Zowel theoretische bronnen als praktijkfeedback (bijvoorbeeld van de CISO) gaven aan dat bijna-incidenten waardevolle inzichten bieden voor preventie en risicomanagement. Dit leidde tot een verduidelijking van bijna- incidenten in de procedure.

5.2.2 Conflicten tussen theorie en praktijk

Hoewel er veel overeenkomsten zijn, waren er ook conflicten tussen theoretische richtlijnen en praktische haalbaarheid:

Complexe juridische terminologie: De wettelijke vereisten bevatten termen die moeilijk te begrijpen zijn voor niet-technisch personeel. Om dit te verhelpen, is een definitielijst met uitleg van de definities toegevoegd.

Prioritering van incidenten: De theorie benadrukt het belang van het melden van alle significante incidenten, maar in de praktijk werd aangegeven dat de beschikbare middelen beperkt zijn. Dit conflict is opgelost door specifieke meldingscriteria te definiëren (bijvoorbeeld incidenten met directe impact op patiëntenzorg).

Verantwoordelijkheden tussen teams: De theorie vraagt om een duidelijke verdeling van verantwoordelijkheden, maar tijdens de feedbacksessies bleek dat er binnen het ziekenhuis nog onduidelijkheid bestond over wie verantwoordelijk is voor specifieke taken. Dit werd opgelost door aan te geven dat het Security Team van het ziekenhuis coördineert.

5.2.3 Keuzes en prioritering

De gemaakte keuzes zijn gebaseerd op de balans tussen juridische naleving en praktische toepasbaarheid:

Naleving boven operationele efficiëntie: Bij conflicten is prioriteit gegeven aan juridische naleving, bijvoorbeeld door het opnemen van expliciete meldcriteria en verplichtingen.

Praktische bruikbaarheid als randvoorwaarde: De procedure moest werkbaar blijven voor het ziekenhuispersoneel. Dit leidde tot visuele hulpmiddelen zoals een definitielijst en het vereenvoudigen van taalgebruik.

Aanpassing op basis van feedback: Keuzes werden herzien op basis van input uit feedbacksessies, zoals de toevoeging van een verduidelijking over bijna-incidenten met een potentieel risico en de verduidelijking van verantwoordelijkheden.

5.3 Conclusie

De centrale onderzoeksvraag luidt:

> *Welke ontwerpeisen zijn, na een analyse van de uit de NIS 2- richtlijn voortvloeiende verplichtingen voor cyberincident meldingen binnen zorginstellingen, relevante wet- en regelgeving, vakliteratuur op het gebied van informatiebeveiliging, kennis en ervaringen van interne betrokkenen binnen het Martini Ziekenhuis, en feedback op de procedurebeschrijving, relevant voor de procedurebeschrijving aangaande de meldplicht voor cyberincidenten binnen het Martini Ziekenhuis?*

Op basis van de analyse kunnen de volgende definitieve ontwerpeisen worden geformuleerd. Ten eerste is het van essentieel belang dat de verantwoordelijkheden van betrokkenen, zoals de Privacy Officer, CISO en TSO, duidelijk worden vastgelegd. Dit omvat ook de toewijzing van bevoegdheden bij complexe beslissingen, zoals het escaleren van incidenten. Ten tweede moeten de meldingscriteria expliciet en helder zijn. Incidenten met potentiële schade moeten worden opgenomen in de meldplicht, met een gestandaardiseerd stappenplan dat duidelijk omschrijft wie wanneer moet worden geïnformeerd en welke vervolgstappen nodig zijn. Daarnaast moeten de procedurebeschrijvingen voldoen aan de technische en juridische vereisten van de NIS2-richtlijn, AVG en relevante normen zoals NEN7510 en ISO27001. Dit betekent onder andere dat bijna-incidenten of potentiële schade ook worden geregistreerd om een volledig beeld te krijgen van het dreigingslandschap. Communicatie is een ander belangrijk aandachtspunt. De procedure moet toegankelijk zijn voor alle medewerkers, inclusief niet-technisch personeel, en om vindbaar te zijn worden opgenomen in het kwaliteitsportaal van het MZH. Om consistentie te waarborgen, moeten complexe termen worden vertaald naar begrijpelijke taal. Tot slot is het noodzakelijk om een systeem van periodieke training en audits te implementeren. Regelmatige simulaties en trainingen zorgen ervoor dat medewerkers adequaat voorbereid zijn op cyberincidenten, terwijl audits en evaluaties helpen om de procedure up-to-date te houden en te optimaliseren.

Lijst van veel voorkomende afkortingen en begrippen

AP: Autoriteit Persoonsgegevens
AVG: Algemene Verordening Gegevensbescherming
Cbw: Cyberbeveiligingswet
CISO: Chief Information Security Officer
CSF: Cybersecurity Framework
CSIRTs: Computer Security Incident Response Teams
DORA: Digital Operational Resilience Act
EDPB: European Data Protection Board
FG: Functionaris Gegevensbescherming
GDPR: General Data Protection Regulation
ITIL: Information Technology Infrastructure Library
ISMS: Information Security Management System
MZH: Martini Ziekenhuis
NIS2: Network and Information Security Directive
TSO: Technisch Security Officer
UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming
Wbni: Wet beveiliging netwerk- en informatiesystemen
WGBO: Wet op de Geneeskundige Behandelingsovereenkomst

Bronnenlijst

Van Aardenne & Barensen 2023
H. van Aardenne & J. Barensen, ‘NIS2: nieuwe regels tegen cyberaanvallen’, *Adv.bl. 2023/2041,* afl. 5, p. 78-81.

Brouwer & van Mil 2023
N. Brouwer & J. van Mil, ‘Cybersecurity in Europa’, *Njb 2023/674,* afl. 10, p. 748-757.

Cybersecuritybeeld Nederland 2023
‘Cybersecuritybeeld Nederland’, www.nctv.nl, 2023.

ENISA Threat landscape 2021
ENISA. ‘ENISA Threat Landscape. 2021’, www.enisa.europa.eu, 2021.

Fg informatie 2024
‘Fg-informatie’, www.autoriteitpersoonsgegevens.nl, 2024.

Gal-Or & Ghose 2005
E. Gal-Or & A. Ghose, ‘*The economic incentives for sharing security information’,* Inform Syst Res 2005, p.186–208.

Gordon, Loeb & Lucyshyn 2003
L. Gordon, M. Loeb M & W. Lucyshyn, ‘*Sharing information on computer systems security: an economic analysis’*, J Account Public Pol 2003, p. 461– 85.

IT Ausfall unikllinik Dusseldorf 2020
‘IT-Ausfall an der uniklinik Dusseldorf’, www.uniklinik-dusseldorf.de, 2020.

Jacobs & Jansen 2024
B.P.F. Jacobs & R.H.T. Jansen, *‘Hoe hackers vastlopen’ Computerrecht* 2024/3, afl. 1, p. 15-17.

Kolby, Morrow & Zbierek 2022
P.R. Kolby, M.R.Morrow & L. Zabierek, '*The cybersecurity risks of an escalating Russia–Ukraine conflict',* Harvard Business Revieuw 2022. www.hbr.org.

Kranenborg & Verhey 2023
H.R. Kranenborg & L.F.M Verhey, '*Melding 'Datalekken'', SBR Wetenschap* 2024/11.5.2. P. 11.

Kwaliteit en onderzoek 2024
'Kwaliteit en onderzoek', www.martiniziekenhuis.nl, 2024.

Nctv 2024
Nctv, nis2-richtlijn, 2024 www.nctv.nl.

Nis2-richtlijn 2024
'nis2-richtlijn', www.digitaleoverheid.nl, 2024.

Over de autoriteit persoonsgegevens 2024
'Over de autoriteit persoonsgegevens', www.autoriteitpersoonsgegevens.nl, 2024.

Over het Martini Ziekenhuis 2024
'Over het Martini Ziekenhuis', www.martiniziekenhuis.nl, 2024.

Overzicht van alle onderwerpen 2024
'Overzicht van alle onderwerpen/nis2-richtlijn' www.digitaleoverheid.nl , 2024.

Praat 1998
J.C. van Praat, '*Information Tehtnologies Infrastucture Libary (ITIL)',* Handboek EDP-Auditing, 1998, Par. 3.6.2.

Privacyverklaring 2024
'Privacyverklaring', www.werkenbijmartiniziekenhuis.nl, 2024.

Samen werken aan patiëntveiligheid 2024
'Samen werken aan Patiëntveiligheid', www.martiniziekenhuis.nl, 2024.

Soorten rechtshandelingen 2024
'Soorten rechtshandelingen', www.european-union.europa.eu, 2024.

Steenbrugge 2024
W. Steenbrugge, '*internetconsulatie Cyberbeveiligingswet', Computerrecht* 2024/144, p. 302.

Toepassing van EU-wetgeving 2024
'Toepassing van EU-wetgeving', www.commission.europa.eu, 2024.

Veenstra 2024
K. Veenstra, *'Nis2 checklist'*, www.hbo-kennisbank.nl, 2024.

Viergever & van Til 2023
L. Viergever & G. van Til, 'NIS2 en de AVG', *Computerrecht 2023/116.*

Wat de ICT afdeling kan doen 2019
'Wat de ICT- Afdeling kan doen', www.digivaardigindezorg.nl, 2019.

Wat gaat de NIS2-richtlijn betekenen voor uw organisatie? 2024
'Wat gaat de nis2-richtlijn betekenen voor uw organisatie?', www.ncsc.nl, 2024.

Wat is een honeypot 2024
'Wat is een honeypot', www.kaspersky.nl, 2024.

WBNI 2024
'Wbni', www.wetten.overheid.nl, 2024.

Welke sectoren vallen onder de NIS2-richtlijn 2024
'Welke sectoren vallen onder de NIS2-richtlijn', www.nctv.nl, 2024.

Ziekenhuizen, Martini Ziekenhuis 2024
'Ziekenhuizen, Martini Ziekenhuis', www.ziekenhuischeck.nl, 2024.

Overige bronnen:

Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet).

Richtlijn (EU) 9/2022 on personal data breach notification under GDPR.

De Cyber Resilience Act

Stel je een wereld voor waarin steeds meer alledaagse apparaten — van je slimme thermostaat tot industriële machines — verbonden zijn met het internet. Deze digitale producten maken ons leven gemakkelijker en efficiënter, maar brengen ook risico's met zich mee. Want hoe weet je als consument of als bedrijf of deze apparaten wel voldoende beveiligd zijn tegen hackers of datalekken? Precies daar komt deze nieuwe wetgeving om de hoek kijken. De Europese Unie constateerde een groeiend probleem: digitale producten kwamen massaal op de markt, maar er golden nauwelijks duidelijke en afdwingbare regels over hun cyberveiligheid.

Op 10 oktober 2024 heeft de Raad van de Europese Unie goedkeuring gegeven aan de Cyber Resilience Act (hierna: CRA). Deze nieuwe Europese verordening, gericht op fabrikanten, distributeurs en importeurs van hardware en software, moet ervoor zorgen dat digitale producten in Europa veiliger worden. Zowel tijdens de ontwikkeling als gedurende hun levenscyclus.[1] De CRA is op 10 december 2024 in werking getreden en is gericht op hardware en software die vanaf 11 december 2027 op de Europese markt wordt gebracht. De nieuwe wet stelt bindende eisen aan de cyberveiligheid van digitale producten die in de Europese Unie worden verkocht, waaronder software en Internet of Things-apparaten (IoT). Dit zorgt ervoor dat consumenten en bedrijven veilig gebruik kunnen maken van digitale producten, denk aan webcams en smart-tv's die deel uitmaken van het IoT. De CRA maakt onderdeel uit van een brede digitale Europese strategie, waaronder ook de NIS II-richtlijn valt.[2]

Alle fabrikanten, importeurs, distributeurs en gebruikers van producten met digitale elementen krijgen te maken met de CRA. De meeste verplichtingen gelden voor fabrikanten. Zij dragen integraal de verantwoordelijkheid voor een veilig product. Ook voor importeurs geldt dat ze in moeten staan voor de veiligheid van het product, en actief moeten controleren of producten wel aan de CRA voldoen. Brengt een importeur het product onder zijn eigen merk op de markt? Dan wordt de importeur beschouwd als fabrikant, en gelden alle plichten die ook op een fabrikant van toepassing zijn.[3]

1 'Europese Raad keurt Cyber Resilience Act goed', digitaleoverheid.nl.
2 'De Cyber Resilience Act treedt vandaag in werking', digitaltrustcentrer.nl.
3 'Cyber Resilience Act (CRA)', rdi.nl.

Een Europese verordening heeft een andere werking dan een Europese richtlijn (zoals hiervoor de NIS2-richtlijn). Een verordening is namelijk rechtstreeks van toepassing in alle lidstaten, zonder dat nationale wetgeving nodig is om de regels in werking te laten treden. Zodra een verordening is aangenomen en gepubliceerd, heeft zij overal in de Europese Unie dezelfde juridische kracht en werking, en moeten burgers, bedrijven en overheden zich er direct aan houden. In tegenstelling tot een richtlijn, die eerst omgezet moet worden in nationale wetgeving, zorgt een verordening voor uniformiteit binnen de Europese Unie voorkomt zij verschillen in de uitvoering tussen lidstaten.

Uit de CRA vloeien een viertal kernverplichtingen voort, waarbij niet naleving van de verplichtingen kan leiden tot een sanctie vanuit de (Europese) toezichthouder. De eerste verplichting houdt in dat fabrikanten producten ontwikkelen waarbij tijdens de ontwerpfase, ontwikkelfase en productiefase rekening wordt gehouden met de cybersecurityvereisten zoals opgenomen in bijlage I van de CRA. Deze Bijlage I bevat een lijst met een tiental punten waar in detail wordt beschreven op welke manieren de producten moeten worden gefabriceerd. Cybersecurity kan daarmee door fabrikanten niet meer als bijzaak worden gezien, maar moet door de komst van de CRA als kerntaak worden beschouwd.

Naast het ontwerpen, ontwikkelen en produceren van producten zijn fabrikanten op grond van de CRA ook verplicht om kwetsbaarheden vast te stellen, te documenteren en te verhelpen door middel van beveiligingsupdates. Deze verplichting brengt met zich mee dat fabrikanten verantwoordelijk zijn voor de gehele cybersecurity van hun product gedurende de gehele levenspanne ervan. Het vereist een proactieve rol, waarbij de fabrikant op eigen initiatief op zoek gaat naar kwetsbaarheden en deze pijnpunten actief aanpakt. Daarnaast moeten fabrikanten op grond van de CRA informatie verstrekken over de beveiligingsrisico's van hun producten en hoe consumenten deze risico's kunnen beheren. Het kan daarbij bijvoorbeeld gaan om de consument te adviseren updates door te voeren, zich niet te verbinden met kwaadwillende netwerken of om regelmatig een virusscan uit te voeren. Tot slot moeten fabrikanten op grond van de CRA ervoor zorgen dat hun producten altijd conformeren aan de algemeen geldende Europese normen voor (digitale) producten, voordat zij op de markt komen.

Het laatste afstudeeronderzoek wat in dit boek wordt gepresenteerd is gemaakt door en (inmiddels alumni) van de opleiding HBO-Rechten van de Hanze. In zijn onderzoek stond de CRA centraal. Het doel van zijn onderzoek was het opleveren van een beroepsproduct, waarin de keuze is gemaakt voor een beslisboom. De beslisboom heeft als doel om mkb- bedrijven te helpen bij het vaststellen van de verplichtingen op grond van de CRA. Het onderzoek bestaat uit een theoretisch deel, waarin de inhoud en achtergrond van de CRA worden geanalyseerd en een praktijkdeel, waarin de beslisboom wordt getest en verbeterd op basis van interviews met ondernemers. Uiteindelijk zijn er twee versies van de beslisboom ontwikkeld — een analoge en een interactieve — waarmee het mkb beter voorbereid is op de implementatie van de CRA.

mr. P. M. Piest
mr. dr. T. Mulder

De Cyber Resilience Act voor het MKB

Coen Veenstra

Samenvatting

In dit onderzoek wordt de Cyber Resilience Act (hierna: “CRA”) voor het mkb besproken, met als doel een beslisboom te ontwikkelen die helpt bij het bepalen van de verplichtingen en vereisten onder de nieuwe wetgeving. Het onderzoek omvat zowel een theoretisch als een praktisch deel om een beroepsproduct te maken.

Het theoretisch onderzoek richt zich op de achtergrond en de inhoud van de CRA. Deze wetgeving, voorgesteld door de Europese Unie, beoogt een geharmoniseerd beveiligingsniveau voor digitale producten te waarborgen. De verordening is een reactie van Europa op de toenemende cyberdreigingen zoals de Pegasus spyware en de WannaCry ransomware.

De CRA stelt dat fabrikanten verantwoordelijk zijn voor de cyberbeveiliging gedurende de hele levenscyclus van hun producten en verplicht hen om beveiligingsupdates te verstrekken.
In het theoretisch kader worden verschillende belangrijke aspecten van de CRA besproken, waaronder de essentiële eisen, het territoriale toepassingsgebied en de procedures voor conformiteit. Ook wordt ingegaan op de uitzonderingen en de specifieke verplichtingen voor verschillende soorten producten en bedrijven. Een groot onderdeel is de mogelijkheid van een vermoeden van conformiteit op basis van geharmoniseerde normen, zoals beschreven in rapporten van de *European Union Agency for Cybersecurity* (ENISA).

Het praktijkonderzoek bestaat uit interviews en een pilot/test van het beroepsproduct. Deze interviews zijn voornamelijk gericht op kleinere ondernemingen die onder de verzwaarde verplichtingen van de CRA vallen of die zich in specifieke juridische situaties bevinden. De feedback uit deze interviews helpt bij het aanpassen en verbeteren van de beslisboom.

Tijdens de tests is de beslisboom geëvalueerd op gebruiksvriendelijkheid en duidelijkheid, waarbij methoden zoals *Tree Testing* zijn gebruikt. De resultaten wijzen erop dat het belangrijk is om de CRA in hoofdlijnen te presenteren, omdat uitgebreide details vaak nog nader uitgewerkt moeten worden door de EU. Het is voor het mkb daarom van belang om het minimale te doen om aan de wetgeving te voldoen en zich te concentreren op de belangrijkste verplichtingen en procedures.

Op basis van de feedback uit de praktijk en de theorie zijn de definitieve ontwerpeisen vastgesteld, op basis waarvan zowel een analoge als een interactieve versie van de beslisboom is ontwikkeld. Deze versies complementeren elkaar de analoge versie is geschikt voor fysieke presentaties, terwijl de interactieve versie online toegankelijk is en meer uitleg kan geven bij de stappen. Dit zorgt ervoor dat het mkb beter voorbereid is op de implementatie van de CRA, met een nuttig en duidelijk hulpmiddel om de eisen en verplichtingen te herkennen en begrijpen.

De conclusie van het onderzoek stelt dat het niet realistisch is om alle verplichtingen, vereisten en definities volledig in de beslisboom te verwerken. In plaats daarvan, wordt de CRA in hoofdlijnen besproken en worden de belangrijkste gevolgen en procedures benoemt. Zodra de CRA definitief in werking treedt kan dit onderzoek als een basis worden gebruik.

1. Inleiding

1.1 Contextsanalyse

De opdrachtgever van dit onderzoek is Trix Mulder, een lector bij het Lectoraat Juridische Aspecten van Ondernemerschap. Het Lectoraat Juridische Aspecten van Ondernemerschap onderzoekt complexe juridische vraagstukken op strategisch en tactisch niveau die voor (sociale) ondernemers relevant zijn. Het doel van het lectoraat is wet- en regelgeving beter aan te laten sluiten op de behoeften van ondernemers.

Het lectoraat doet samen met ondernemers, docenten en studenten onderzoek naar thema's rondom het vergroten van de sociale impact van mkb in de regio, aanbestedingen met sociale voorwaarden en coöperatie- vorming. Daarnaast draagt het lectoraat bij aan vraagstukken op het terrein van *governance*, publiek-private samenwerking en cybersecurity.

De focus van het praktijkgericht juridisch onderzoek van het lectoraat richt zich op:

1. **Digitale transformatie**: praktische ondersteuning bieden voor ondernemers en (semi-) publieke organisaties bij juridische vraagstukken rondom digitale toepassingen.
2. **Impact ondernemerschap**: de versterking van ondernemen met impact door de werking van wet- en regelgeving wordt onderzocht vanuit het perspectief van ondernemers, waarbij de nadruk ligt op eigen beslissingsruimte voor ondernemers en het voorkomen van regeldruk.
3. **Governance**: versterking van de onderlinge regionale samenwerking van ondernemers en de samenwerking met de overheid, met de nadruk op (Europees) aanbestedingsrecht, coöperatieve vorming en publiek-private samenwerking.[1]

Als lector is de opdrachtgever verantwoordelijk voor het leiden van onderzoek binnen dit specifieke vakgebied, met een focus op de juridische aspecten die relevant zijn voor ondernemers en ondernemerschap. De functie omvat het initiëren, coördineren en uitvoeren

1 H. Groningen, 'Juridische Aspecten van Ondernemerschap | Hanze', www.hanze.nl, 27 september 2023.

van onderzoeksprojecten, het begeleiden van onderzoekers en studenten, en het delen van de onderzoeksresultaten met de academische gemeenschap en het bedrijfsleven. Gezien de omvang van het lectoraat zijn er geen specifieke afdelingen of teams.

Ook is bij deze specifieke opdracht de projectgroep Cybersecurity Noord-Nederland (hierna: “CSNN”) relevant. De opdrachtgever werkt namelijk, met dit onderzoek, samen met deze groep in het kader van dit project. CSNN is een samenwerking van organisaties in Noord-Nederland met als doel om bij te dragen aan de bewustwording van het gevaar van cybercriminaliteit en samen met de ondernemers in Noord- Nederland te werken aan een betere cyberweerbaarheid.[2]

De aanleiding voor het lectoraat en CSNN om deze afstudeeropdracht uit te laten voeren is de nieuwe Europese verordening de CRA. De verordening heeft rechtstreekse werking en is aangekondigd in de 2020 *EU Cybersecurity Strategy*.[3] Deze strategie heeft als doel, het waarborgen van *global and open Internet*. De EU probeert namelijk aan de hand van wetgevings-, investerings- en beleidsinitiatieven de fundamentele rechten en beveiliging van *global and open Internet* voor alle Europese inwoners te waarborgen. De CRA bouwt verder op andere wetgevingen inzake cybersecurity, in het bijzonder de NIS2 richtlijn.[4]

Deze wetgeving wordt beschouwd als relevant en potentieel problematisch voor mkb-ondernemers die producten of software met digitale componenten fabriceren, distribueren of importeren in Europese lidstaten.

Het probleem dat het lectoraat en CSNN willen oplossen, is dat veel ondernemers mogelijk niet op de hoogte zijn van de (nieuwe)verplichtingen die zullen voortvloeien uit de CRA. Dit gebrek aan duidelijkheid kan leiden tot onzekerheid over wat er van hen wordt verwacht en kan resulteren in overtredingen van de nieuwe verordening. Dit heeft potentieel nadelige gevolgen. De toezichthouder kan bijvoorbeeld een product van de markt halen[5], een geldboete opleggen[6] of andere sancties opleggen als niet aan de verplichtingen wordt.

Naast de opdrachtgever zijn de ondernemers die vallen onder het besluit: “een gemeenschappelijk kader voor het verhandelen van producten in de EU”[7] relevant voor het onderzoek, zij zijn immers gehouden aan de CRA. Voor hen is het van cruciaal belang om op de hoogte te zijn van de verplichtingen die voortvloeien uit de CRA, om naleving van de verordening te waarborgen en potentiële negatieve consequenties te vermijden.

2 ‘Over ons – Cyber Security Noord Nederland’, https://cybersecurity-noord.nl.
3 ‘The Cybersecurity Strategy | Shaping Europe’s digital future’, https://digital-strategy.ec.europa.eu, 2 februari 2024.
4 ‘Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe’s digital future’, https://digital-strategy.ec.europa.eu, 2 februari 2024.
5 Artikel 43 lid 4 CRA.
6 Artikel 53 CRA.
7 Besluit nr. 768/2008/EG — een gemeenschappelijk kader voor het verhandelen van producten in de EU.

Ook is het reeds genoemde project CSNN relevant. Het lectoraat voert dit onderzoek immers uit in het kader van dit project.[8] Omdat het onderzoek wordt uitgevoerd in het kader van dit project, zal het onderzoek gericht zijn op mkb-bedrijven in Noord-Nederland.

Zowel het lectoraat als CSNN hebben nog geen specifieke maatregelen genomen om dit probleem aan te pakken. Daarom is deze afstudeeropdracht aangeboden om het vraagstuk in kaart te brengen en duidelijkheid te verschaffen over de verplichtingen die voortvloeien uit de CRA voor de mkb-ondernemers.

Met dit onderzoek, wil het lectoraat een gedetailleerd overzicht bieden van de verplichtingen die voortvloeien uit de CRA voor mkb-ondernemers in Noord-Nederland, met als doel hen te helpen bij het begrijpen en naleven van de nieuwe verordening. Dit zou het lectoraat in staat stellen om de benodigde kennis over te dragen aan de mkb-ondernemers in Noord-Nederland, zodat zij potentiële overtredingen kunnen voorkomen en de juridische risico’s te minimaliseren die gepaard gaan met het niet voldoen aan de CRA.

1.2 Beroepsproduct

Een beslisboom om te zien of de mkb-ondernemingen in Noord-Nederland voldoen aan de nieuwe verplichtingen van de CRA ten opzichte van andere wetgevingen, standaarden en normen op dit gebied:

Hier wordt een duidelijk overzicht gegeven van verplichtingen en eisen van de CRA. Het kan zijn dat bepaalde ondernemingen geen veranderingen zullen tegenkomen omdat ze al compliant zijn, bijvoorbeeld op basis van een verzwaarde ISO-norm of dergelijke in de markt bekende normen en standaarden. Of dat er juist nieuwe verplichtingen voortvloeien die nog niet in soortgelijke wetgeving is opgenomen. Om duidelijk te maken of er iets veranderd voor de ondernemingen (en of ze dus stappen dienen te ondernemen) is een beslisboom een geschikte optie. Zo kunnen de ondernemers via de stappen in de beslisboom gecategoriseerd worden in de toepasselijke groepen gedefinieerd in de CRA. De verplichtingen voor deze groepen kunnen vervolgens worden vergeleken met de verplichtingen uit soortgelijke wetgeving waaraan de ondernemers al voldoen. Zo komt duidelijk in beeld voor de betrokkenen welke specifieke verplichtingen en eisen zij nog niet aan voldoen.

Er is gekozen voor een (digitale) interactieve beslisboom zie voorbeelden, dit kan met verschillende programma’s, zoals *Typeform* of *Google Forums*. Er zijn namelijk veel doodlopende stappen in de boom, dit als gevolg van de overlap met andere cybersecuritywetgeving en de CRA. Deze doodlopende stappen zorgen ervoor dat er niet veel ruimte overblijft bij een analoge versie. Een interactieve optie is dermate overzichtelijker. Bovendien zorgt de interactieve versie ervoor dat bij elke stap ook nog uitleg/advies kunnen worden gegeven. Gezien het lectoraat een gedetailleerd overzicht wil bieden is dit een belangrijk aspect. Indien dit niet mogelijk blijkt zal er een analoge versie worden gemaakt of ten minste een blauwdruk voor de beslisboom, dan wel een combinatie van de versies.

8 ‘CyberSecurity Noord-Nederland’, www.digitalsocietyhub.nl, 13 april 2022.

1.3 Verantwoording beslisboom

Om vast te stellen welk beroepsproduct geschikt is voor dit onderzoek is samen met de stakeholders zoals het lectoraat en CSNN afgestemd wat het doel is van een dergelijk product. Zij willen een duidelijk en gedetailleerd overzicht voor mkb-bedrijven in Noord-Nederland, over de specifieke verplichtingen en eisen die de CRA aan deze bedrijven oplegt. Hierna is een lijst met meerdere opties opgeleverd als uitwerking van dit doel. Hieruit is gekozen voor de voornoemde beslisboom. De andere opties zijn nog in een te vroeg stadium nu de CRA zelf nog niet definitief is. Er moet immers eerst gekeken worden of er überhaupt verplichtingen voortvloeien voor de mkb-ondernemers, voordat deze verplichtingen worden ingevuld. De andere opties zoals een conformiteitsbeoordeling of een stappenplan om compliant te zijn, zijn namelijk al invullingen van dergelijke verplichtingen, terwijl deze verplichtingen er nog niet zijn voor het mkb. De beslisboom kan echter op een toegankelijke wijze aangeven of de CRA nieuwe verplichtingen en eisen zal opleggen en hierbij een overzicht geven wat deze zijn.

Zoals reeds vermeld zal dit onderzoek gericht zijn op mkb-bedrijven in Noord-Nederland. Zij zullen dan ook de eindgebruikers zijn van de beslisboom. Bovendien zal de beslisboom gedistribueerd worden vanuit het netwerk van CSNN, de aangesloten groep van ondernemers bij dit project zullen in ieder geval gebruik maken van de beslisboom.

1.4 Ontwerpeisen

De eerste beschrijvingen van de ontwerpeisen zijn nog rand voorwaardelijk, naarmate het onderzoek zullen nader ontwerpeisen voortvloeien of juist, indien van toepassing, eisen worden afgebakend. Ook wat betreft de vormgeving en bruikbaarheid eisen zullen nadere eisen worden geïdentificeerd door de gebruikers van het beroepsproduct. Uit de eerste gesprekken met de opdrachtgever vloeien wel al eerste eisen voort:

Inhoudelijk

- Het beroepsproduct moet de specifieke verplichtingen en eisen die voortvloeien uit de (CRA) nauwkeurig en volledig weergeven. Dit omvat het identificeren en uitleggen van alle relevante bepalingen en voorschriften binnen de CRA die van toepassing zijn op mkb-bedrijven in Noord- Nederland. Het is van essentieel belang dat het beroepsproduct alle relevante aspecten van de CRA behandelt om volledige naleving van de wet te garanderen.
- Het beroepsproduct moet specifieke aandacht besteden aan de unieke kenmerken en uitdagingen van mkb-bedrijven in Noord-Nederland. Dit omvat het identificeren van regionale aspecten die relevant zijn voor de CRA-naleving, zoals lokale marktomstandigheden, culturele verschillen, en economische factoren. Door de relevantie voor de lokale context te waarborgen, wordt het beroepsproduct praktisch en direct toepasbaar voor mkb-ondernemers in Noord-Nederland. Dit is van essentieel belang gezien het kader van dit onderzoek als deel van het project CSNN.
- Het beroepsproduct moet de volledige reikwijdte van de CRA dekken. Dus niet enkel fabrikanten maar alle groepen van de die vallen onder de bepalingen van de verordening.

Vormgeving

- De vormgeving van het beroepsproduct moet gebruiksvriendelijk zijn voor mkb-bedrijven. Opnieuw gelet op het kader van dit onderzoek als deel van het project CSNN, moet het beroepsproduct toegankelijk zijn voor de kleinere ondernemingen in Noord-Nederland. Denk hierbij aan vertaling van juridisch taalgebruik, duidelijke indeling van de informatiestructuur, het weghalen van gebruiksdrempels die voortvloeien uit achtergrond, vaardigheden of eventuele beperkingen van de gebruikers. De nadere invullingen van deze gebruiksvriendelijkheid zal worden achterhaald aan de hand van de test van het beroepsproduct bij de mkb-ondernemingen. De feedback van de ondernemers die het beroepsproduct gaan gebruiken is ook van belang voor de vormgeving.
- Ook is het een wens voor de opdrachtgever om meerdere versies van het beroepsproduct te zien. Dit om zowel een actieve vorm van feedback en aanpassingen toe te passen als om actualiteit te garanderen. Het is namelijk mogelijk dat er nog nader tekstuele aanpassingen zullen komen in de CRA door het parlement, zij dienen nog te buigen over de huidige versie van de verordening.

1.5 Voorbeelden

Interactieve versies

- Een zelf evaluatie van Rijksoverheid voor de NIS2 richtlijn.
- Een cyberweerbaarheid scan als voor beeld voor het geven van uitleg bij de stappen.

Analoge versie

- Een beslisboom van Rijksoverheid voor de *single use plastics*-richtlijn.

1.6 Wet- en regelgeving

Als eerst is uiteraard de CRA[9] zelf van belang voor het beroepsproduct, nu het onderzoek en het beroepsproduct gaan over de eisen en verplichtingen die voortvloeien uit deze verordening. De CRA verhoudt zich en verwijst zelf ook naar andere EU-wetgeving en voorstellen, namelijk de Algemene verordening gegevensbescherming (hierna: “AVG”)[10], en de voorstellen voor de AI-verordening[11] en de herziene Netwerk- en informatiebeveiligingsrichtlijn (Hierna: “NIS2).[12] Zoals reeds vermeld valt de CRA onder de *2020 EU Cybersecurity Strategy*. Dit plan van de EU heeft dan ook verschillende wetten en voorstellen, die deels overlappen met de CRA, waardoor deze ook relevant zijn voor het onderzoek en beroepsproduct.

9 Voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020.

10 Verordening (EU) 2016/679 bescherming natuurlijke personen i.v.m. verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

11 Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de Unie.

12 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).

Ook naar de herziende verordening inzake algemene productveiligheid (VAPV)[13] betreffende risico's die voortvloeien uit nieuwe technologieën, wordt verwezen in de CRA.
Naast deze verordeningen geeft de CRA in artikel 16 aan dat de Algemene Productaansprakelijkheidsrichtlijn[14] een aanvulling is op de CRA. De CRA zelf is gericht op productveiligheid ten opzichte van de aansprakelijkheid waar deze richtlijn op is gericht.

Tot slot kan het relevant zijn om naar soort gelijke (sectorale)wet- en regelgeving te kijken. Denk hierbij aan bijvoorbeeld *de Radio Equipment Directive, Machinery Directive* en *de automotive Directive*. De CRA geeft veelal zelf aan dat dergelijke producten kunnen vallen onder zowel haar toepassingsbereik als die van de sectorale regelgeving.[15] Nederland verwelkomt de CRA als een belangrijke bouwsteen naast bestaande of toekomstige wet- en regelgeving.[16] Daarom is het voor dit onderzoek ook relevant om naar deze, wet- en regelgeving te kijken.

Het is de bedoeling om een duidelijk beeld te geven van de wisselwerking en overlap die de CRA heeft met de bovenstaande regelgeving, echter zullen deze slechts kort aangestipt worden. De CRA verwijst immers zelf naar de regelgeving en licht toe in hoeverre deze relevant is of bepaalde groepen uitsluit van haar eisen en verplichtingen. Het onderzoek zal zich dan ook primair focussen op de bepalingen en eisen van de CRA. Dit is met uitzondering van de toepasselijke artikelen en bijlagen van de NIS-2 richtlijn, omdat deze richtlijn net als de CRA van cruciaal belang is in de in de *2020 EU Cybersecurity Strategy*. Deze overlap met de NIS2 ziet, in het kader van dit onderzoek, voornamelijk op het verschil tussen diensten- en producten waarop cyberbeveiligingseisen worden gesteld.

1.7 *Best practices* en eerder onderzoek

Omdat de CRA een relatief nieuw voorstel is, is het eerder onderzoek voornamelijk verkennend van aard. Deze onderzoeken gaan hoofdzakelijk in op de CRA in hoofdlijnen en waar de kritiekpunten liggen. Er is in eerder onderzoek niet veel geschreven over mkb-ondernemingen, terwijl dit onderzoek is juist gericht op de mkb- ondernemingen in Noord-Nederland. Uit eerder onderzoek is wel bruikbare informatie te halen over de eisen en verplichtingen van de CRA en wat de knelpunten zijn van de verordening. Dit betreft informatie over de inhoud van de CRA. Daarnaast is er diepgaand onderzoek over wisselwerking en overlap van cybersecuritywetgeving en in de markt bekende normen en standaarden.

Dit onderzoek zal zelf de gevolgen voor het mkb moeten definiëren aan de hand van de CRA.

1.8 Beperkingen

Het onderwerp van dit onderzoek betreft een voorstel voor een verordening. Deze is dan ook niet definitief en kan nog worden aangepast. Dit aspect kan zowel de scope als de conclusies van het onderzoek beïnvloeden. Bovendien richt het onderzoek zich specifiek op het mkb in Noord-Nederland, wat kan betekenen dat niet alle groepen van de CRA kunnen worden opgenomen in het praktijkonderzoek. Het is namelijk mogelijk dat niet alle fabrikanten importeurs en distributeurs, die vallen onder de scope van de CRA, vertegenwoordigd zijn in het mkb van Noord-Nederland. Deze beperking kan de generaliseerbaarheid van de resultaten beïnvloeden, omdat de CRA een breder perspectief vertegenwoordigt.

1.9 Onderzoeksdoel en -vragen

1.9.1 Onderzoeksdoelstelling

Het doel van dit onderzoek is het opleveren van een beslisboom inzake de verplichtingen en eisen die voortvloeien uit de CRA voor Het Lectoraat Juridische Aspecten van Ondernemerschap in het kader van het project CSNN zodat dit kan worden gebruikt door mkb-ondernemingen in Noord-Nederland die producten of software met digitale componenten produceren, importeren of distribueren, dat voldoet aan de toepasselijke wettelijke vereisten vanuit de CRA en relevante wet- en regelgeving, parlementaire stukken en (juridische) vakliteratuur, rekening houdend met inzichten van de praktijkervaring van ondernemers op het gebied van het implementeren van Europese verordeningen en rekening houdend met de huidige werkwijze van de ondernemers inzake cybersecurity en wat is afgestemd op een test van een concept van de beslisboom van toepassing bij de ondernemers?

1.9.2 Centrale onderzoeksvraag

Welke ontwerpeisen zijn na een analyse van de toepasselijke wetsartikelen en bijlages uit de CRA, relevante wet- en regelgeving, parlementaire stukken en (Juridische)vakliteratuur en met inzichten van de ondernemers op het gebied het implementeren van Europese verordeningen voor mkb-ondernemingen en met een analyse van de huidige werkwijze van de ondernemers inzake cybersecurity, en een test van een concept van de beslisboom bij de ondernemers?

1.9.3 Theorie- en praktijkdeelvragen

Theorie

Welke ontwerpeisen voor de beslisboom vloeien voort uit de toepasselijke wetsartikelen en bijlages uit de CRA, de herziene NIS2 en (juridische) vakliteratuur m.b.t. de inhoud van de beslisboom?

Welke ontwerpeisen vloeien voort uit parlementaire stukken m.b.t. de inhoud van de beslisboom?

Praktijk

Welke ontwerpeisen voor de beslisboom vloeien voort uit eerdere ervaring met het implementeren van Europese wetgeving door mkb-ondernemers m.b.t. de inhoud van de beslisboom?

13 Voorstel voor een verordening van het Europees Parlement en de Raad inzake algemene productveiligheid, tot wijziging van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 87/357/EEG van de Raad en Richtlijn 2001/95/EG van het Europees Parlement en de Raad, COM(2021) 346 final 2021/0170 (COD).
14 Richtlijn 85/374/EEG betreffende de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen der Lid-Staten inzake de aansprakelijkheid voor producten met gebreken.
15 Toelichting CRA, hoofdstuk 1 achtergrond van het voorstel.
16 Kamerstuken II 2021/22, 21501-33, nr. 900.

Welke ontwerpeisen voor de beslisboom vloeien voort uit een analyse van de huidige werkwijze van de ondernemers inzake cybersecurity m.b.t. de inhoud van de beslisboom?

Welke ontwerpeisen voor de beslisboom zijn af te leiden uit een test van een concept van de beslisboom bij mkb-ondernemers?

2. Methodologische verantwoording

2.1 Theorie

Gezien de CRA een nieuwe verordening betreft, is er nog geen jurisprudentie over. Ook is er niet heel veel geschreven over dit onderwerp, vooral omdat de verordening nog niet definitief is gepubliceerd. Er zijn wel wat bronnen uit Nederland, maar die zijn nog niet erg diepgaand. Dit onderzoek heeft deze wel gebruikt om een compleet beeld te krijgen. Voor meer diepgang, is ook gekeken naar bronnen uit Europa. De belangrijkste gebruikte bronnen in het theoretische kader en waar deze voor zijn gebruikt zijn:

- De Parlementaire stukken van de Europese commissie en -parlement, met name de positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024.

Hier heeft het Europese parlement de nodige toelichting gegeven bij de CRA over bepaalde bepalingen, definities, reikwijdte etc. Misschien wel het belangrijkste is hier ook de proportionaliteit voor het mkb besproken en wat de EU voor hen gaat doen m.b.t compliance van deze verordening. Gezien het onderzoek gericht is op het mkb is dit een belangrijke bron.

- De meest diepgaande juridische vakliteratuur is Burri & Zihlmann Zeitschrift für Europarecht 2023 en Chiara, International Cybersecurity Law Review 2022/3.

Er zijn meerdere gepubliceerde artikelen in juridische tijdschriften gebruikt voor het theoretisch kader, maar deze waren veruit het meest diepgaand en uitgebreid. Bovendien worden in vele bronnen verwezen naar deze artikelen als voetnoot en bron. Daarmee blijken dit de experts op literatuur voor de CRA. Deze tijdschriften zijn gebruikt voor een diepere uitleg en voorbeelden over de CRA, ter verduidelijking van haar bepalingen en inhoud. Bijvoorbeeld bij de definities van het territoriale toepassingsgebied, voorbeelden bij de bijzondere gevallen van artikel 15/16 CRA en verduidelijking van de essentiële vereisten uit de CRA.

- De ENISA rapporten met name H. Ramos e.a, *Cyber Resilence Act Requirements Standards Mapping.*

Zoals bij hoofdstuk 1 besproken was voorafgaand aan het theoretisch onderzoek de vraag of het kan zijn dat bepaalde ondernemingen al voldoen aan de vereisten van de CRA. Bijvoorbeeld op basis van een ISO-norm of andere wetgeving op het gebied van cybersecurity. Uit het theoretisch onderzoek bleek dat dit gedeeltelijk kan aan de hand van een vermoeden van conformiteit. Daar kwam juist de vraag uit wanneer hier sprake van is, waarvoor deze bron het belangrijkst was.

De Eu had dezelfde vraag en heeft dit neergelegd bij de European Union Agency for Cybersecurity (hierna: “ENISA”). Zij hebben vervolgens alle geharmoniseerde normen vergeleken met de eisen van de CRA en hier de conclusies van vastgelegd in dit rapport. Deze conclusies waren van belang voor dit onderzoek.

2.2 Praktijk

Voor het praktijkgedeelte van dit onderzoek is gebruik gemaakt van een pilot/test van het beroepsproduct en het afnemen van interviews. Een Interview heeft de voorkeur voor de kleinere specifieke groepen ondernemers die verzwaarde verplichtingen hebben, of juridisch bijzondere situaties. De mogelijkheid van doorvragen en het diepergaand onderzoek van interviewen, kan worden gebruikt om specifieke beleidsstukken van deze groep te achterhalen en de ervaringen rondom deze verzwaarde verplichtingen in kaart te brengen. Tevens is het in dit onderzoek niet realistisch om grote omvang in beeld te brengen, gezien het praktijkonderzoek gefocust is op de bijzondere gevallen en de interessante juridische aspecten die voortvloeien uit de theorie. Dit zijn specifieke groepen ondernemers. Bovendien is dit onderzoek gefocust op een toekomstige wetgeving bij het mkb. Het is daarmee zeer onwaarschijnlijk dat het mkb hier veel ervaring dan wel beleid- of compliance stukken heeft.

De test heeft de voorkeur omdat dit onderzoek een hele specifieke doelgroep heeft. De enige manier om te achterhalen of het beroepsproduct nuttig en duidelijk is voor deze specifieke doelgroep, is op basis van het verhalen van feedback van die doelgroep.

De objecten waren een Fabrikant en distributeur die onder de scope van de CRA vallen. Een distributeur en importeur hebben beide vrijwel dezelfde verplichtingen, het heeft niet vul nut om beide te interviewen gezien het enige voordeel is om het verschil dat de een producten buiten de Europese markt inkoopt en de ander binnen te vergelijken. De bijzondere situaties zoals beschreven in hoofdstuk 3.4.4 zijn voor beide actoren echter hetzelfde, terwijl dit het juridisch interessante aspect van deze actoren is. Tot slot om de scope buiten het materiële toepassingsgebied te testen, is er ook een uitgesloten onderneming als object opgenomen. De selectiecriteria voor de objecten zijn gebaseerd op de juridisch relevante aspecten en de haalbaarheid van het verkrijgen van informatie. Er is altijd gekozen voor de oprichter gezien die aangaf meeste juridische ervaring te hebben en het meest bekend was met technische aspecten van CRA. Relevantie voor juridische aspecten: Denk aan ontwerpeisen die rechtstreeks verband houden met de juridische verplichtingen of uitzondering uit de CRA.

Bijvoorbeeld

- De onderneming Onderneming A is gekozen, omdat het een distributeur van producten met digitale elementen is, die mogelijk ook actief is in nationale veiligheid en de bijzonder gevallen van artikel 15/16 CRA.
- De onderneming Onderneming B is gekozen, gezien de overlap met de Ai verordening en om de scope van software als een product met digitale elementen compleet te maken.
- De onderneming OmniDrone is gekozen, om een volledig beeld te krijgen van een uitgesloten ondernemer en de stappen die leidden tot een uitsluiting van de CRA te testen bij de beslisboom.

Toegankelijkheid van informatie: Dit omvat bijvoorbeeld het vermogen om toegang te krijgen tot relevante documenten zoals beleidsnotitie en werkprocessen of andere interne documentaties. Het is dus ook afhankelijk van het netwerk en wie wil meewerken aan het onderzoek dan wel het project CSNN. Zo zijn er tientallen ondernemingen benaderd die uiteindelijk niet wouden meewerken of waar het praktisch niet uitkwam. In dat opzicht is het belangrijk te melden dat het niet gebruikelijk is voor mkb-ondernemers om actief te zijn in cybersecurity, naast het minimale wat van hen wordt vereist. Hetgeen wat leidt tot minder onderzoeksobjecten aangezien er ook geen informatie toegankelijk is.

Gezien met voornoemde objecten een volledige scope wordt gevuld zijn ze toepasbaar voor alle deelvragen.

De interviews zijn opgezet met een vragenlijst waarbij aansluitend de pilot test is gedaan. Zo kan de feedback voor het beroepsproduct ook direct worden besproken. Aangezien de onderzoeksobjecten hetzelfde bleven is dit de meest logische keuze. De test is opgezet aan de hand de methode *Tree Testing*[17], op deze manier is er een methodische aanpak om te zien of de beslisboom juiste conclusies en duidelijke vragen oplevert.[18] Voor de interview vragen lijst is gekozen, omdat er voorafgaand het praktijkonderzoek duidelijke onderzoek punten waren die uit de theorie voortvloeiden. Elk object had zijn eigen interessante aspecten die op deze manier overzichtelijk in kaart konden worden gebracht. Wat betreft overkoepelende thema’s was het mogelijk om algemene vragen te stellen, zoals bij de deelvraag m.b.t. eerdere ervaringen rondom wetgeving. Hiermee kon op dezelfde vraag van meerdere stakeholders antwoorden worden vergeleken.

2.3 Beroepsproduct

In dit onderzoek is gebruik gemaakt van de zelfevaluatie van de NIS2 van de Rijksoverheid als voorbeeld voor het beroepsproduct.[19] Deze keuze is gemaakt op basis van de relevantie en betrouwbaarheid van de bron. De zelfevaluatie van de Rijksoverheid is gebaseerd op de NIS2, een vergelijkbare Europese wetgeving die ook betrekking heeft op cybersecurity.

17 W.L. in R.-B.U. Experience, ‘Tree Testing: Fast, Iterative Evaluation of Menu Labels and Categories’, www.nngroup.com.
18 Zie hoofdstuk 4.3.1 voor meer informatie.
19 Zie hoofdstuk 1.5 de Nis-2 zelfevaluatie.

Beide beroepsproducten hebben als doel organisaties te helpen bepalen of ze onder de desbetreffende wetgeving vallen en wat de gevolgen daarvan zijn. Dit sluit nauw aan bij het doel van dit onderzoek, waardoor het een passend voorbeeld is voor de beslisboom.

Er zijn geen geschikte *best practices* gevonden die even relevant en betrouwbaar zijn als de zelfevaluatie van de Rijksoverheid. Er is uitgebreid gezocht naar vergelijkbare evaluatietools, maar de andere voorbeelden zijn enkel als inspiratie gebruikt voor de vormgeving.

Sterke en zwakke punten
Sterke punten van het beroepsproduct zijn het diepgaande theoretische onderzoek en de brede scope die gebruikt zijn bij het ontwikkelen van de beslisboom. Dit maakt het een goede basis als eerste stap bij de CRA, omdat het een uitgebreid overzicht biedt van alle vereisten en verplichtingen die in de wetgeving staan. Als er echter nog amendementen komen, kan het onderzoek gemakkelijk worden aangepast en verder worden uitgewerkt op basis van de al uitgezochte theoretische aspecten. Een zwak punt is de relatief kleine doelgroep van het onderzoek, wat invloed heeft gehad op de omvang en representativiteit van het praktijkonderzoek. Zoals beschreven in hoofdstuk 1.8, kan het onderzoek generaliserend zijn, maar het behandelt wel de volledige scope van de CRA en het beroepsproduct is uitgebreid getest. Een andere beperking is dat de CRA nog niet in werking is getreden, wat betekent dat sommige aspecten van de wetgeving mogelijk nog veranderen.

Definitieve Ontwerpeisen
Bij de verwerking van de definitieve ontwerpeisen in het beroepsproduct is zorgvuldig gekeken naar de resultaten van zowel het theorie- als praktijkonderzoek. Deze ontwerpeisen zijn vervolgens vertaald naar een beslisboom die zowel in analoge als interactieve vorm beschikbaar is. Er is ook rekening gehouden met de wens van het mkb om het minimale te doen om aan de wetgeving te voldoen. Hierdoor is besloten om de CRA in hoofdlijnen te presenteren en niet alle verplichtingen, vereisten en definities volledig uit te werken. In plaats daarvan wordt gefocust op de belangrijkste gevolgen en procedures, zoals beschreven in hoofdstuk 5. Een belangrijke ontwerpeis was dat de beslisboom duidelijk maakt wanneer er sprake kan zijn van een vermoeden van conformiteit of uitsluiting van een bepaalde product of verordening. Dit is echter nog niet uitgebreid uitgewerkt, omdat de EU nadere uitvoeringsbesluiten en richtlijnen hierover nog moet publiceren, zoals het geval is bij *lex specialis* artikel 2 lid 4 CRA. Daarom wordt deze mogelijkheid genoemd, maar wordt tevens uitgelegd dat hier nog verdere uitleg over komt.

Inschatting van het beroepsproduct
Er is zowel een analoge versie als een interactieve versie van de beslisboom opgeleverd. Deze versies complementeren elkaar: de analoge versie is geschikt voor fysieke presentaties en biedt overzichtelijkheid, terwijl de interactieve versie online toegankelijk is en een interactieve gebruikerservaring biedt. Dit sluit aan bij de wensen van de opdrachtgever en de definitieve ontwerpeisen. Hierdoor is het beroepsproduct bruikbaar voor het mkb in de praktijk, echter is het nog steeds een vroeg stadium. De CRA zal mogelijk nog veranderingen ondergaan en blijf het de vraag of de CRA überhaupt definitief in werking treedt. Zodra de CRA wel definitief wordt na eventuele amendementen, kan de beslisboom opnieuw beoordeeld en verder verbeterd worden om te blijven voldoen aan de wensen van het mkb. Het advies van dit onderzoek is dan ook om de beslisboom en het onderzoek zelf als basis te gebruiken voor diepgaandere ontwikkeling wanneer de CRA in een nieuw stadium zal komen.

3. Ontwerpeisen vanuit de theorie

3.1 Totstandkoming van de verordening

3.1.1 Europa

Er is op dit moment geen (Europese) wetgeving die bepaalt dat economische actoren digitale producten moeten beveiligen.[20] Hoewel dit natuurlijk niet betekent dat digitale producten altijd onvoldoende beveiligd zijn, wil de Europese wetgever minimumeisen vaststellen om het beveiligingsniveau te harmoniseren. Digitale hardware- en softwareproducten vormen namelijk een van de belangrijkste wegen voor succesvolle cyberaanvallen. In een verbonden omgeving kan een cybersecurity-incident in één product een hele organisatie of een hele toeleveringsketen beïnvloeden, vaak over de grenzen van de interne markt heen binnen enkele minuten.[21] Voorbeelden van dergelijke aanvallen die de Unie nu met de CRA tracht te voorkomen zijn:

- *The Pegasus spyware*, die kwetsbaarheden in mobiele telefoons heeft misbruikt.[22]
- *The WannaCry ransomware*, die een Windows-kwetsbaarheid heeft misbruikt, waardoor computers in 150 landen zijn getroffen.[23]

Bekende soortgelijke wetgeving van de Unie en nationaal niveau betrof slechts gedeeltelijk de geïdentificeerde cybersecurity-gerelateerde problemen en risico's, waardoor een wetgevend lappendeken ontstond binnen de interne markt.[24] Om voornoemde reden is door de Europese wetgever de CRA voorgesteld. De CRA zal ervoor zorgen dat producten met digitale elementen die in de EU op de markt worden gebracht veilig(er) zijn, fabrikanten verantwoordelijk blijven voor de cyberbeveiliging gedurende de hele levenscyclus van een product en consumenten de nodige bescherming genieten.[25]

20 ENISA, Opinion Consumers and IoT security, 2019. P.5.
21 Voorstel CRA, Achtergrond van het voorstel, toelichting bij de CRA: Motivering en doel van het voorstel.
22 'European Cyber Resilience Act (CRA)', www.european-cyber-resilience-act.com.
23 Idem.
24 Brouwer & Reijneveld, Cybersecurity in Europa , afl. aflevering 10. H.1.
25 Voorstel CRA, Achtergrond van het voorstel, toelichting bij de CRA: Motivering en doel van het voorstel.

Hiermee worden twee belangrijke problemen aangepakt die kosten toevoegen voor gebruikers en de samenleving zowel in de zin van zuivere vermogensschade, als in de zin van schade aan zaken of zelfs aan personen:

- het lage niveau van cybersecurity van producten met digitale elementen, zoals blijkt uit wijdverspreide kwetsbaarheden en de ontoereikende en inconsistente verstrekking van beveiligingsupdates om ze aan te pakken;
- en een ontoereikend begrip en toegang tot informatie door gebruikers, waardoor ze niet in staat zijn om producten te kiezen met adequate cybersecurity-eigenschappen of om ze op een veilige manier te gebruiken.[26]

3.1.2 Doelen en Inhoud

De CRA heeft vier specifiek geformuleerde doelstellingen om de bovenstaande problemen aan te pakken. De CRA zal namelijk met horizontale werking:

i) ervoor zorgen dat fabrikanten de beveiliging van producten met digitale elementen verbeteren vanaf de ontwerp- en ontwikkelingsfase en gedurende de gehele levenscyclus;
ii) zorgen voor een samenhangend cyberbeveiligingskader, waardoor naleving voor hardware- en softwarefabrikanten gemakkelijker wordt;
iii) de beveiligingskenmerken van producten met digitale elementen transparanter maken; en
iv) bedrijven en consumenten in staat stellen om producten met digitale elementen veilig te gebruiken.

Om deze doelen te bereiken bevat de CRA:[27]

- regels voor het in de handel brengen van producten met digitale elementen;
- cybersecurityeisen voor het ontwerp, de ontwikkeling en de productie van producten met digitale elementen;
- vereisten voor de procedures inzake de respons op kwetsbaarheden.

Deze bovenstaande aspecten komen aanbod in dit onderzoek. Zo zullen de eisen en regels worden behandeld in hoofdstuk 3.4 en de procedures hiervoor in hoofdstuk 3.6. Er zal echter eerst behandeld worden welke producten onder de scope van de CRA vallen en welke juist uitgesloten zijn.

3.2 Scope

3.2.1 Materiaal

De CRA heeft een breed materieel toepassingsgebied, het is van toepassing is op producten met digitale elementen waarvan het beoogde of redelijkerwijs voorzienbare gebruik een directe of indirecte logische of fysieke gegevensverbinding met een apparaat of netwerk omvat.[28] Een logische of fysieke gegevensverbinding, houdt in dat het product op een manier toegang heeft tot gegevens c.q. informatiesystemen. Producten met digitale elementen zijn, elk software- of hardware product en de oplossingen voor gegevensverwerking op afstand, met inbegrip van software- of **hardwarecomponenten** die **afzonderlijk** in de handel worden gebracht.[29] Gezien de wetgever hier software als een losstaand product beschouwt, kan software ook vallen onder de regelgeving van de CRA.[30]

Bovendien lijkt de CRA niet alleen “voltooide” software- en hardware producten te omvatten, maar ook de onderdelen daarvan. Zo blijkt uit de definitie **componenten** die **afzonderlijk** in de handel worden gebracht.[31] Dientengevolge omvat het toepassingsgebied niet alleen eindapparaten, maar ook onderdelen. Voorbeelden van dergelijke producten die dus onder de scope vallen zijn:[32]

Tabel 5

Eindapparaten	Software	Componenten
laptops	firmware	computerprocessoreenheden
smartphones	besturingssystemen	videokaarten
sensoren en camera’s	mobiele apps	softwarebibliotheken
slimme robots	desktoptoepassingen	
slimme kaarten	videospellen	
slimme meters		
mobiele apparaten		
slimme luidsprekers		
routers		
switches		
industriële controlesystemen.		

Over het algemeen omvat de CRA in feite alle producten met digitale elementen en wordt het ook wel gezien als de verordening inzake *Internet of Things*(hierna: “IoT”). IoT wordt simpel gedefinieerd als, alle apparaten die met internet verbonden zijn[33], dit sluit dan ook aan bij de bovenstaande definitie, gegevensverbinding met een apparaat of netwerk, die de CRA geeft voor digitale elementen.

De omvangrijke toepassingsgebied lijkt goed gerechtvaardigd, aangezien potentieel alle producten met digitale elementen die geïntegreerd zijn in of verbonden zijn met een groter elektronisch informatiesysteem, kunnen dienen als een toegangspunt voor aanvallen.[34] Bovendien benadrukt de Europese Commissie (hierna: “Commissie”) dat kwetsbaarheden niet alleen worden gevonden in eindproducten, maar ook in tussenliggende softwarecomponenten. De Commissie neemt dus het standpunt op deze allesomvattende benadering langs de

26 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024.
27 Brouwer & Reijneveld, Cybersecurity in Europa , afl. aflevering 10. H.2.1.
28 Artikel 2 lid 1 CRA.
29 Artikel 3 lid 1 CRA.
30 Overweging 46 CRA.
31 Overweging 37 CRA.
32 ‘European Cyber Resilience Act (CRA)’, www.european-cyber-resilience-act.com.
33 ‘Beveiligingstips voor Internet of Things (IoT) | Digital Trust Center (Min. van EZK)’, www.digitaltrustcenter.nl.
34 Overweging 7 CRA.

lijnen van, de cybersecurity van het hele ecosysteem wordt alleen gegarandeerd als al zijn componenten beveiligd zijn.[35]

3.2.2 Territoriaal

De CRA bevat geen expliciete bepalingen over het territoriale toepassingsgebied. Echter wordt er in bepaalde overwegingen en artikelen vaak verwezen naar producten met digitale elementen die “op de EU-markt worden geplaatst” of “beschikbaar worden gesteld op de markt”.[36] Dit geeft aan dat de CRA van toepassing is op dergelijke producten die te koop worden aangeboden of worden gebruikt in de Unie. Dit is met name relevant bij artikel 1 sub a CRA “regels ***voor het in de handel brengen van***”.[37] Alhoewel er door de wetgever dus niet expliciet regels inzake het territoriaal toepassingsgebied zijn opgenomen, kan men wel spreken van een dergelijke scope.

Relevant is om te noemen dat de CRA bij de verschillende definities van de verschillende economische actoren, bij de definitie van de fabrikant, in tegenstelling tot die van de importeur en distributeur, geen verwijzing naar de Unie bevat. Dit lijdt dat een fabrikant buiten de EU in beginsel niet aan de verplichtingen van de CRA hoeft te voldoen. Alhoewel fabrikanten de veiligheidseisen van de CRA zouden kunnen negeren als ze buiten de Unie zijn gevestigd, mogen importeurs niet een van deze producten op de Europese markt importeren. Importeurs moeten immers verklaren dat de producten van fabrikanten voldoen aan de eisen van Bijlage I van de CRA.[38]

Met andere woorden, de reikwijdte van de verordening strekt zich uit buiten de grenzen van de EU, aangezien elke fabrikant buiten de EU die exporteert naar EU-lidstaten gehouden is aan de wetgeving, in de zin dat de importeur en (in mindere mate) de distributeur verantwoordelijk zijn voor hun naleving. Zij mogen een product immers niet op de markt brengen als deze niet compliant is met de gestelde eisen.

3.3 Uitsluitingen

De scope van de CRA is dus behoorlijk omvangrijk, er zijn echter ook producten die worden uitgesloten van de verplichtingen uit de verordening. Dit kan op basis van soort gelijke (sectorale)wet- en regelgeving, letterlijke uitsluitingen genoemd in de CRA of op basis van een vermoeden van conformiteit. Het laatste hiervan zal nader worden uitgewerkt met betrekking tot welke gevolgen dit heeft voor de verplichtingen in hoofdstuk.

3.3.1 Uitsluitingen toepassingsgebied

Uit artikel 2 CRA vloeien bepaalde letterlijk uitgesloten gevallen van het toepassingsgebied voort. Zoals de verordeningen van lid 2 jo. lid 3:

- **Verordening (EU) 2017/745 betreffende medische hulpmiddelen:**
  Men hoeft niet aan de vereisten van de CRA te voldoen wanneer het in de handel brengen, het op de markt aanbieden en de ingebruikneming van medische hulpmiddelen voor menselijk gebruik betreft. Klinisch onderzoek naar dergelijke hulpmiddel ook uitgesloten. Dergelijke producten dienen te voldoen aan de vereisten van de verordening inzake medische hulpmiddelen.
- **Verordening (EU) 2017/746 betreffende medische hulpmiddelen voor in-vitrodiagnostiek.**
  Dit is in vergelijking met vorige verordening inzake medische hulpmiddelen ook uitgesloten voor medische hulpmiddelen in ivd’s. Oftewel diagnostische testen hoeven ook niet aan de vereisten van de CRA te voldoen, wanneer een economische actoren het in de handel brengen of het aanbiedt op de markt.
- **Verordening (EU) 2019/2144 betreffende motorvoertuigen:**
  Ook de motorvoertuigen van de categorieën M, N en O, zoals gedefinieerd in artikel 4 van Verordening (EU) 2018/858, en op systemen, onderdelen en technische eenheden die voor dergelijke voertuigen worden ontworpen en gebouwd zijn uitgesloten van de CRA. Dus als het een van de volgende voortuigen is of onderdeel is van dergelijke voortuigen is het uitgesloten van de verplichtingen uit de CRA.[39] Denk hierbij niet alleen aan voertuigen als eindproducten, maar ook aan software of componenten van voertuigen met digitale elementen.
- **Verordening (EU) 2018/1139 betreffende burgerluchtvaart:**
  Vrijwel alles wat te maken heeft met luchtvaart en het leveren van software of eindproducten in deze sector is uitgesloten van de CRA. Zie artikel 2 van de verordening inzake gemeenschappelijke regels op het gebied van burgerluchtvaart. Als een product een (type)certificaat heeft van deze verordening, dan is het product uitgesloten van de vereisten van de CRA. Het product dient in een dergelijk geval wel te voldoen aan de vereisten van de verordening betreffende burgerluchtvaart.

Al deze verordeningen worden letterlijk uitgesloten, omdat de Commissie deze acht als *lex specialis* voor de CRA. Oftewel speciale wetgeving die voorrang heeft op algemene wetgeving. In dit geval dient de CRA *als lex generalis*. Artikel 2 lid 4 CRA geeft de voorwaarden voor wanneer de Commissie dergelijke regelgeving *als lex specialis* acht, namelijk producten met digitale elementen die vallen onder andere voorschriften van de Unie waarvan de essentiële eisen overeenkomen met die van Bijlage I CRA indien:

- het strookt met het algemene regelgevingskader dat op die producten van toepassing is. Dit betekent dat eisen van een andere regelgeving overeenkomen met de eisen van de CRA. Het mag dus niet zo zijn dat de eisen van andere regelgeving lichter zijn dan die van de CRA. Een voorbeeld hiervan is
- En (cumulatief) als deze eerdere eisen hetzelfde beschermingsniveau biedt. (oftewel als de verplichtingen minder zwaar zijn zou een product alsnog aan de CRA-verplichtingen moeten voldoen).

35 Burri & Zihlmann 2023. P.B17.
36 Artikel 3 lid 20,21,22 jo. 23 CRA.
37 Chiara, International Cybersecurity Law Review 2022/3. P.260.
38 Burri & Zihlmann 2023. P.B25, zie ook hoofdstuk 3.4.2.
39 Zie productie 1 voor dergelijke voertuigen.

Wat onder artikel 2 lid 4 CRA valt is niet definitief verwoord in de CRA, maar de Commissie behoudt de bevoegdheid om dergelijke gevallen vasttestellen/wijzigen[40], met een vermelding van welke producten en regels dit dan zijn. Denk hierbij aan sectorale regelgeving en uitvoeringsbesluiten.

Tot slot vloeit uit artikel 2 lid 5 CRA nog een letterlijke uitsluitingsgrond voort. De CRA is niet van toepassing op producten die uitsluitend bedoeld zijn voor nationale veiligheid of militaire doeleinden. Ook producten die ontworpen zijn voor verwerking van gerubriceerde informatie. Gerubriceerde informatie is vertrouwelijke informatie van de EU en ziet vaak op veiligheid/ beveiliging.[41] In dit licht wijst de CRA wel uitdrukkelijk naar de term uitsluitend. Een groot deel van de producten die in de defensiesector worden gebruikt, zijn namelijk civiele en *dual-use* producten met digitale elementen, en zijn dus niet uitsluitend bedoeld voor defensie. Producten die dus niet uitsluitend nationale veiligheid of militaire doelen dienen, zijn wel onderworpen aan de CRA.[42]

3.3.2 Opensource software

Vrije en *opensourcesoftware* die buiten het kader van een handelsactiviteit wordt ontwikkeld of geleverd zijn ook uitgesloten van de CRA.[43] *Open source software stewards* spelen een rol bij de bepaling van dergelijke gevallen, er komt hier namelijk nogal wat bij kijken. *Open source software stewards* zijn bepaalde stichtingen en entiteiten die vrije en open-source software ontwikkelen en publiceren in een zakelijke context, zoals non- profitorganisaties die vrije en open-source software ontwikkelen in een zakelijke context.[44]

De CRA definieert geen relevante termen zoals “vrije software”, “*open-source software*” en “vrije en *open- source software*”. Bovendien is de reikwijdte van “commerciële activiteit” onduidelijk, aangezien volgens deze overweging een commerciële activiteit niet alleen kan worden gekenmerkt door het in rekening brengen van een prijs voor een product, maar bijvoorbeeld ook door het in rekening brengen van een prijs voor technische ondersteuningsdiensten.

Als een fabrikant dus *open source software* gebruikt/op de markt brengt en onder commerciële activiteit valt, zal hij onder de scope van de CRA vallen. Het is daarom van belang om aan te tonen of er sprake is van commerciële activiteit met de opensource software, bijvoorbeeld middels integratie voor een product dat wordt verkocht.[45]

40 Artikel 50 lid 2 CRA.
41 ‘Bescherming van gerubriceerde EU-informatie (EUCI)’, www.consilium.europa.eu.
42 Burri & Zihlmann 2023.P.B18.
43 Overweging 10 CRA.
44 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024. Overweging 19.
45 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024. Overweging 18 jo. 19.

3.3.3 AI-systemen

Indien producten met digitale elementen, die ook kunnen worden aangemerkt als AI-systemen met een hoog risico, binnen het toepassingsbereik van de CRA vallen en voldoen aan de in de CRA voorgeschreven eisen, worden die producten geacht in overeenstemming te zijn met de in de AI-verordening vastgestelde cyberbeveiligingseisen.[46] AI-systemen zijn uitgesloten zolang ze aan de juiste conformiteit beoordelingsprocedures en eisen hebben voldaan van de AI verordening.[47] Artikel 43 van de AI-verordening heeft immers voorrang boven de respectievelijke bepalingen van de CRA met betrekking tot de conformiteitsbeoordelingsprocedures met betrekking tot de essentiële cybersecurityvereisten van Bijlage I.[48]

Deze uitsluiting geldt echter niet voor de kritieke producten die zijn opgenomen in Bijlage III van de CRA. In een dergelijk geval is de voorgeschreven procedure artikel 24 CRA van toepasing. Dit moet alleen op de essentiële eisen van de CRA Bijlage I. Dergelijke andere eisen moeten ook nog via de procedure van AI verordening.

3.3.4 Vermoeden van conformiteit

Enkele genoemde gevallen van uitsluiting zien niet op een complete uitsluiting, maar op een uitsluiting op basis van een zogeheten ‘vermoeden van conformiteit’. Een vermoeden van conformiteit ziet op overlap met geharmoniseerde normen. Het kan zijn dat bepaalde procedures en werkwijze in plaats zijn waarmee al voldaan is aan de essentiële eisen van de CRA Bijlage I. Dan kan de fabrikant spreken van een vermoeden van conformiteit.[49]

Dit is het geval bij:

- **Machineproducten zoals genoemd in artikel 9 van verordening (EU) 2023/1230**
  Al hoewel zowel de CRA als de Machineproducten Verordening vallen onder dezelfde scope met overlappende cybersecurity eisen, moeten dergelijke overeenkomsten aangetoond worden door de fabrikant. Dit valt dus onder een vermoeden van conformiteit en zal door een *standarisation* proces gedaan kunnen worden. Zolang de eisen daadwerkelijk op hetzelfde niveau zijn als artikel 2 lid 4 CRA.
- **Producten met een Cyberbeveiligingscertificatie afgegeven door Verordening (EU) 2019/881**
  Dit ziet op een vermoeden van conformiteit op basis van cyberbeveiligingscertificering die vrijwillig uit bovenstaande verordening voortvloeien. Gezien de CRA een voorstel is en nog geen definitieve wet, is ook nog niet definitief wanneer er sprake is van een vermoeden van conformiteit op basis van een cyberbeveiligingscertificering afgegeven door deze verordening. Een dergelijke certificatie zal nog moeten worden gemaakt door ENISA, de organisatie die bevoegd is om dergelijke certificatie aftegeven.

46 Artikel 8 lid 1 jo. Artikel 15 AI-verordening.
47 Artikel 8 lid 1 CRA.
48 Chiara, International Cybersecurity Law Review 2022/3. P.266.
49 Zie tevens hoofdstuk 3.5.

3.3.5 Software as a Service

Tot slot is de herziende NIS2 richtlijn nog relevant. Deze richtlijn regelt namelijk de conformiteit inzake cyberbeveiliging voor diensten. Zoals eerder vermeld, ziet de CRA op producten met digitale elementen die op de markt worden gebracht. Het leveren van *software* als een dienst of *software as a service* (hierna: “SaaS”) wordt dan ook in beginsel uitgesloten van de CRA. SaaS is het ter beschikking stellen van software als een online dienst, vaak in de vorm van een licentie. De NIS2 ziet gericht op het waarborgen van een hoog niveau van cyberbeveiliging van diensten in de kort gezegd kritieke infrastructuur.[50] De toepasselijkheid van NIS2 is ook de reden dat SaaS niet valt onder de CRA. De wetgever beoogt om de technische specificaties en maatregelen die vergelijkbaar zijn met de essentiële cyberbeveiligingsvereisten van de CRA, ook worden ingevoerd bij SaaS middels de NIS2. Deze wetgeving dienen dan ook complementair te zijn, waardoor men nog steeds kan spreken van geharmoniseerde standaarden.[51]

Overweging 9 stelt echter dat SaaS wel onder de CRA valt indien het:

- Oplossingen voor gegevensverwerking op afstand zijn, die zijn gekoppeld aan een product met digitale elementen bedoeld voor normale gegevensverwerking op afstand en;
- Als de software is ontworpen en ontwikkeld door of onder de verantwoordelijkheid van de fabrikant van het betrokken product en;
- Bij gebreke waarvan een dergelijk product met digitale elementen een van zijn functies niet zou kunnen vervullen.

Gegevensverwerking op afstand wordt als volgt gedefinieerd: elke gegevensverwerking op afstand waarvoor de software is ontworpen en ontwikkeld door de fabrikant of onder de verantwoordelijkheid van de fabrikant, en bij gebreke waarvan het product met digitale elementen een van zijn functies niet zou kunnen vervullen.[52]

Wat dit betekent is dat SaaS enkel onder de CRA valt als het product en de bijbehorende software zodanig met elkaar zijn verbonden dat het product een van zijn functies niet kan uitoefenen zonder de software, mits dezelfde fabrikant zowel het product met digitale elementen ontwikkelt als de software ontwikkelt of laat ontwikkelen.

Ter verduidelijking heeft de Commissie dit geschreven in haar overwegingen:

> *Richtlijn (EU) 2022/2555 (NIS2) is van toepassing op cloudcomputingdiensten en cloudservicemodellen, zoals Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) of Infrastructure-as-a-Service (IaaS).*[53]

50 Toelichting achtergrond voorstel CRA onder 1. Kritieke infrastructuur ziet op organisaties actief in sectoren van essentieel belang zoals onderwijs-, overheid- of de financiële sector.
51 Overweging 5 en 9 CRA.
52 Artikel 3 sub 2 CRA.
53 Europese Commissie 2022/0272(COD), 20 December 2023.

Tevens bevat NIS2 geen verwijzingen naar de CRA en noemt SaaS ook slechts één keer in overweging 33. Uit de NIS2 volgt in ieder geval niet zonder meer dat de NIS2 niet van toepassing is op software waarop ook de CRA van toepassing is. Wel volgt uitdrukkelijk uit de NIS2 dat SaaS, en de andere cloudcomputingdiensten zoals hierboven beschreven, onder cloudcomputingdiensten vallen. Dit is dan ook conform de definitie in de markt geharmoniseerde ISO/IEC 17788:2014-norm.[54]

3.4 Verplichtingen en eisen CRA

Nu duidelijk is welke producten onder de scope vallen van de CRA, zal vervolgens toegelicht worden wat de verplichtingen en eisen zijn voor partijen die onder deze scope vallen. Zoals reeds beschreven bevat de CRA regels voor het in de handel brengen van producten met digitale elementen met inbegrip van cybersecurityeisen voor het ontwerp, de ontwikkeling en de productie. Dit betekent dat er niet alleen verplichtingen en eisen voortvloeien voor bedrijven die producten met digitale elementen maken, maar ook voor bedrijven die dergelijke producten enkel in de handel brengen. Oftewel zowel fabrikanten, importeurs als distributeurs worden door de CRA aangemerkt als marktdeelnemers die aan haar verplichtingen en eisen zijn onderworpen.[55] Voor al deze groepen zijn verschillende regels die in dit hoofdstuk respectievelijk zullen worden toegelicht.

3.4.1 Fabrikanten

Vrijwel de grootste groep van de CRA en de groep met de meeste verplichtingen en eisen zijn de fabrikanten.[56] Dit is dan ook de eerste partij in de levenscyclus van het product en degene die het product ontwerpen en fabriceren.[57] De letterlijke definitie van een fabrikant is: ‘een natuurlijke of rechtspersoon die producten met digitale elementen ontwikkelt of vervaardigt of die producten met digitale elementen laat ontwerpen, ontwikkelen of vervaardigen, en die onder zijn naam of merknaam in de handel brengt, al dan niet tegen betaling.’[58]

De verplichtingen voor fabrikanten zijn te verdelen in ex ante verplichtingen (voorafgaand aan het op de markt brengen van de producten) en ex post verplichtingen (verplichtingen gedurende de levensduur van het product). De CRA introduceert hiermee een wettelijke verplichting tot *security by design*.[59]

Ex ante

Wellicht de meest belangrijke verplichting is dat een fabrikant alleen een product in handel mag brengen als het is ontworpen, ontwikkeld en geproduceerd overeenkomstig met de essentiële eisen uit Bijlage I afdeling 1 van de CRA ex artikel 10 lid 1. Dit zijn de ex ante verplichtingen.[60]

54 ‘Lexplicatie, Kernbeschrijving bij: Richtlijn (EU) 2022/2555 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn.
55 Artikelsgewijze toelichting CRA, hoofdstuk II.
56 Brouwer & Reijneveld, Cybersecurity in Europa , afl. aflevering 10. H2.2.
57 Idem.
58 Artikel 3 lid 18 CRA.
59 Brouwer & Reijneveld, Cybersecurity in Europa , afl. aflevering 10. H2.3.1.
60 Zie productie 2 voor de essentiële eisen.

Hoewel fabrikanten moeten voldoen aan alle essentiële eisen in verband met de respons op kwetsbaarheden waar de fabrikant rekenen mee moet houden. Moet de fabrikant er ook voor zorgen dat al hun producten worden geleverd zonder bekende kwetsbaarheden die kunnen worden uitgebuit. Zij moeten dus zelf bepalen welke andere essentiële eisen met betrekking tot de productkenmerken relevant zijn voor het betrokken producttype.[61] In dat licht moeten fabrikanten de cyberbeveiligingsrisico's beoordelen die verbonden zijn aan een product met digitale elementen, om betrokken risico's en relevante essentiële eisen vast te stellen en passende geharmoniseerde normen of gemeenschappelijke specificaties toe te passen.[62] Dit betekent dan ook dat de lijst van essentiële eisen niet als een limitatieve lijst gezien moet worden, maar dat fabrikanten een eigen beoordeling moeten doen of de implementatie van deze vereisten op zichzelf leidt tot een passend niveau van cybersecurity van hun product, of dat ze aanvullende maatregelen moeten nemen die specifiek zijn voor de situatie.[63] Dat houdt bijvoorbeeld in dat een fabrikant op eigen initiatief een risicobeoordeling moet doen voorafgaand aan het produceren ex artikel 10 lid 2 CRA.

Met het resultaat van een risicobeoordeling moet de fabrikant rekening houding tijdens de plannings-, ontwerp-, ontwikkelings-, productie-, leverings- en onderhoudsfase van het product. Oftewel: de gehele levenscyclus van het product

Ex post
De ex post verplichtingen vloeien voort uit Bijlage I afdeling 2 CRA. Deze verplichtingen zien op de vereisten voor de respons op kwetsbaarheden. Hierbij kan gedacht worden aan risicobeoordeling, updates, documenteren en het analyseren en bijhouden van bekende problemen/kwetsbaarheden. Deze verplichtingen zien dus op de onderhoudsfase van het product.[64]

Als een fabrikant haar product op de markt wil brengen moet zij een procedure in staat hebben om te beoordelen of aan alle eisen uit Bijlage I zijn voldaan. Dit is een conformiteitsbeoordeling[65] en ze doen dit voor zowel de cyberbeveiligingsrisico's uit afdeling 1 als de procedures voor respons op kwetsbaarheden uit afdeling 2. De CRA schrijft voor dat er een EU-conformiteitsverklaring moet worden opgesteld en een CE-markering op het product moet worden aangebracht.[66] Dit maakt een fabrikant verantwoordelijk voor het vaststellen en verklaren dat het product voldoet aan alle vereisten.

Sommige producten vallen niet onder een eigen risicobeoordeling, maar deze zijn al door de CRA beoordeeld.[67]

61 Burri & Zihlmann 2023. P.B30.
62 Overweging 32 CRA.
63 Burri & Zihlmann 2023. P.B30.
64 Voor meer informatie zie productie 3.
65 Artikel 10 lid 1 CRA.
66 Artikel 10 lid 7 CRA.
67 Dergelijke producten zijn opgenomen in de kritieke lijst van Bijlage III CRA. Met twee afdelingen: klasse I en klasse II producten. zie productie 4 voor meer informatie.

Kritieke producten
Over het algemeen wordt een product als kritiek beschouwd als de negatieve impact van het misbruik van mogelijke cybersecuritykwetsbaarheden in het product ernstig kan zijn vanwege onder andere de functionaliteit met betrekking tot cybersecurity of het beoogde gebruik.[68]

Met name kwetsbaarheden in producten met digitale elementen die een functionaliteit met betrekking tot cybersecurity hebben, zoals beveiligde elementen, kunnen leiden tot een verspreiding van beveiligingsproblemen door de hele toeleveringsketen, waardoor het product kritiek wordt in de zin van de CRA.[69]

Bij de bepaling van het cyberbeveiligingsrisico wordt onder meer rekening gehouden met de aan cyberbeveiliging gerelateerde functionaliteit van het product met digitale elementen en het beoogde gebruik ervan in gevoelige omgevingen, zoals een industriële omgeving.[70] Het onderscheid tussen twee verschillende klassen ziet op de omvang van het risico van het product, waarbij klasse II een groter risico vertegenwoordigt dan klasse I. Ex overweging 27 CRA zal de commissie gedelegeerde handelingen vaststellen om de productcategorieën die vallen onder de klassen I en II van Bijlage III nader te specificeren.

Tot slot kan de Commissie ex overweging 62 jo. artikel 50 CRA de lijst van kritieke producten actualiseren: Om ervoor te zorgen dat het regelgevingskader waar nodig kan worden aangepast, moet aan de Commissie de bevoegdheid worden gedelegeerd om overeenkomstig artikel 290 VWEU handelingen vast te stellen voor het actualiseren van de lijst van kritieke producten van Bijlage III en het specificeren van de definities van deze categorieën producten.

Documenteren en rapporteren
De laatste verplichting voor fabrikanten ziet op documenteren en rapporteren. Een fabrikant dient systematisch te documenteren (dit in verhouding met de hoogte van het risico) over relevante cyberbeveiligingsaspecten met betrekking tot het product gelet op kwetsbaarheden.

Zo moeten een fabrikant een technische communicatie leveren zoals beschreven in Bijlage II CRA.[71] Hierin moet de fabrikant beschrijven hoe haar product werkt en wat de gebruiker het beste kan doen om het product veilig te houden. Dit is een kort overzicht van wat de fabrikant in de technische documentatie moet opnemen[72]:

68 Overweging 25 CRA.
69 Idem.
70 Artikelsgewijze toelichting CRA, hoofdstuk I.
71 Artikel 10 lid 10 CRA.
72 Zie productie 5 voor meer informatie.

Tabel 6

Onderdeel	Informatie
Fabrikantinformatie	Naam, handelsnaam of merknaam van de fabrikant, contactgegevens (postadres en e-mail)
Cyberbeveiligingscontactpunt	Contactpunt voor informatie over cyberbeveiligingskwetsbaarheden
Productidentificatie	Identificatie van het product (type, partij, versie, serienummer) en gebruikersinstructies
Beoogd Gebruik	Beoogd gebruik en essentiële beveiligingskenmerken van het product
Bekende Risico's	Bekende of voorzienbare omstandigheden die significante cyberbeveiligingsrisico's kunnen veroorzaken
Softwarestuklijst	Informatie over de softwarestuklijst en waar deze te raadplegen is
EU-conformiteitsverklaring	Internetadres voor de EU-conformiteitsverklaring
Technische Ondersteuning	Soort technische beveiligingsondersteuning en duur van de ondersteuning"
Gedetailleerde Instructies	• Noodzakelijke maatregelen voor veilig gebruik, • Invloed van veranderingen in het product op gegevensbeveiliging, • Installatie van veiligheidsrelevante updates, • Veilige buitenbedrijfstelling en verwijdering van gebruikersgegevens

In enkele gevallen dat fabrikanten haar risicobeoordeling van het product moet bijwerken en dus de benodigde extra maatregelen moet treffen, als blijkt dat vanwege een bijgewerkt risico het product niet langer voldoet aan de essentiële eisen. De genomen maatregelen moet de fabrikant dan ook delen toelichten aan de gebruiker zodra zij dergelijke maatregelen neemt.[73]

De CRA kent ook een rapportageverplichting dit houdt kort in dat:
Indien fabrikanten een actief gebruikte kwetsbaarheid in hun product ontdekken, of indien zich een incident voordoet dat gevolgen heeft voor de veiligheid van het product, zullen fabrikanten dit moeten melden aan de Europese autoriteit (ENISA) c.q. bij de Nederlandse toezichthouder Rijksinspectie Digitale Infrastructuur (hierna: "RDI").[74] Ook moet de gebruiker onverwijld gemeld worden nadat de fabrikant het ontdekt, als er corrigerende maatregelen zijn moeten deze worden beschreven.[75]

3.4.2 Importeurs

De eerstvolgende partij en de levenscyclus van het product is degen die het product voor het eerst op de markt brengen, oftewel de importeur. De importeur wordt als volgt gedefinieerd in de CRA*: een in de Unie gevestigde natuurlijke of rechtspersoon die een product met digitale elementen in de handel brengt dat de naam of merknaam van een buiten de Unie gevestigde natuurlijke of rechtspersoon draagt;*

De belangrijkste verplichting voor een importeur vloeit voort uit Artikel 13 lid 1 CRA. Importeurs hebben namelijk een verplichting om te controleren of het product voldoet aan de essentiële eisen van Bijlage I. Oftewel het is aan de importeur de taak, voordat een zij een product voor het eerst in de Europese markt introduceren om te beoordeling of een product compliant is aan Bijlage I van de CRA. Dit is dan ook de reeds benoemde territoriale scope die grens overschrijdend beoogt te handelen.

Bovendien hebben importeurs de verplichting om te controleren of de juiste procedure is gevolgd. Dit is van iets onderschikkend belang, maar uiteraard essentiële in het oog van compliance met cyberbeveiligingseisen. Met name in gevallen waar de fabrikant een derde partij dient in te schakelen voor de conformiteitsbeoordelingsprocedures.

Zo moeten importeurs controleren of:
- de fabrikant de technische documentatie heeft opgesteld;
- de fabrikant de juiste conformiteitsbeoordelingsprocedures heeft uitgevoerd;
- en of het product voorzien is van (juiste)CE-markering en technische informatie.

Non compliance
Als een importeur **van mening** is dat niet voldaan is aan de essentiële eisen dan brengt de importeur het product niet in de handel.[76] Bovendien als er een significant cyberbeveiligingsrisico blijkt dan hebben de importeurs ook een rapportageverplichting.[77] Van mening zijn ziet op een vermoeden van de importeur. Importeurs die **niet van mening** zijn dat, maar **weten** of redenen hebben om aan te nemen dat, nemen onmiddellijk de nodige corrigerende maatregelen (oftewel zorg dat de producten wel aan de essentiële eisen van Bijlage I voldoen). Lukt dit niet dan moeten ze het product uit de handel te nemen of terug te roepen.[78]

Bovendien moeten ze in dergelijke gevallen de markttoezichtautoriteiten (voor gevallen binnen Nederland RDI) op de hoogte brengen van non-conformiteit en alle genomen corrigerende maatregelen uitvoerig beschrijven.

Documenteren er rapporteren
Tot slot zijn er ook nog enkele administratieve verplichtingen voor importeurs om aan te stippen. Deze gelden eveneens voor de fabrikanten die onder de CRA vallen. Deze administratieve verplichtingen omvatten het volgende:
- Importeurs vermelden hun naam, geregistreerde handelsnaam of geregistreerde merknaam, het postadres en het e-mailadres op de verpakking of in een bij het product met digitale elementen gevoegd document in gebruikelijke en makkelijke taal.[79]
- Importeurs moeten een exemplaar van de EU-conformiteitsverklaring en de technische documentatie ter beschikking hebben voor de autoriteit, gedurende tien jaar nadat het product in de handel is gebracht. Ook moeten importeurs voldoen aan verzoeken van RDI ter informatie om aan te tonen of fabrikanten haar verplichtingen hebben voldaan.[80]

73 Artikel 10 lid 5 CRA.
74 Artikel 11 lid 1 jo. lid 2 CRA.
75 Artikel 11 lid 4 CRA.
76 Artikel 13 lid 3 CRA.
77 Idem.
78 Artikel 13 lid 6 CRA.
79 Artikel 13 lid 4 CRA.
80 Artikel 13 lid 7 jo. lid 8 CRA.

- In uitzonderlijke gevallen moeten importeurs RDI inlichting als de fabrikant van het geïmporteerde product haar activiteiten stopzet en dus niet aan de *ex post* verplichtingen kan voldoen. Voor zover mogelijk moeten ook de gebruikers van het product worden geïnformeerd.[81]

3.43 Distributeurs

De laatste groep en ook de laatste partij in de productie keten is degene die het product verspreid op de markt. De letterlijke definitie die gegeven wordt voor deze groep is de distributeur: een andere natuurlijke of rechtspersoon in de toeleveringsketen dan de fabrikant of de importeur, die een product met digitale elementen in de Unie op de markt aanbiedt zonder de eigenschappen hiervan te beïnvloeden;

Een voorbeeld ter verduidelijking die het Parlement gaf voor deze groep is:
Het enkele feit van het hosten van producten met digitale elementen op openbare *repositories*, inclusief via pakketbeheerders of op samenwerkingsplatforms, vormt op zichzelf geen terbeschikkingstelling op de markt van een product met digitale elementen. Aanbieders van dergelijke diensten moeten alleen worden beschouwd als distributeurs als zij dergelijke software ter beschikking stellen op de markt en het dus leveren voor distributie of gebruik op de Unie-markt in het kader van een commerciële activiteit.[82]

Het commerciële aspect is heel belangrijk voor de CRA, als een distributeur het product ter beschikking stelt tegen vergoedingen zal hij worden aangemerkt als een distributeur. Distributeurs die een product met digitale elementen op de markt aanbieden, moet de nodige zorgvuldigheid betrachten in verband met de eisen van deze verordening.

Zo moeten zij voordat een product op de markt gaan brengen nagaan of[83]:
- het product met digitale elementen is voorzien van de CE-markering;
- de fabrikant en de importeur hebben voldaan aan de verplichtingen van respectievelijk artikel 10, lid 10, artikel 10, lid 11, en artikel 13, lid 4 CRA.

Het grote verschil is dus dat de importeur de fabrikant controleert en corrigeert of desnoods het product van de markt brengt. Terwijl de distribiteur dit doet voor de importeur en niet de fabrikant. De CRA introduceert hiermee een getrapt systeem.

De distributeur heeft hiermee veel lichtere verplichtingen, dat kan worden verklaard door het feit dat de distributeur het einde van de toeleveringsketen vormt en als zodanig geen relevante invloed heeft op het ontwikkelings-, productie- en upstream distributieproces.

Controleur
Ondanks deze mindere zware verplichtingen, is er nog steeds een belangrijke functie als controleur van het product.[84] De distributeur mag immers een product niet (langer) op de markt brengen als hij gelooft of reden heeft om te geloven dat een product niet voldoet aan de essentiële cybersecurityvereisten. De distributeur moet ook de fabrikant, evenals de markttoezichtautoriteit, informeren als een product een significant cybersecurityrisico met zich meebrengt.[85]

3.4.4 Bijzondere gevallen

Er zijn nog enkele gevallen waar de verplichtingen van fabrikanten van toepassing zijn op importeurs en distributeurs dit vloeit voort uit artikel 15 jo. 16 CRA. Een importeur of distributeur wordt voor de toepassing van deze verordening als een fabrikant beschouwd, wanneer die importeur of distributeur een product met digitale elementen onder zijn naam of merknaam in de handel brengt of een ingrijpende wijziging uitvoert aan het reeds in de handel gebrachte product met digitale elementen.

Er is hier sprake van twee element gezien de wetgever “of” gebruikt. Het eerste element is uniek voor artikel 15 CRA en enkel van toepassing op importeurs of distributeurs. Het tweede element, de ingrijpende wijzigingen, is ook voor rechtspersonen dan wel natuurlijke personen anders dan de importeur en distributeur.

Zie in het licht van het eerste element, onder zijn naam of merknaam in de handel brengt, de definitie van fabrikant: “…..en die onder zijn naam of merknaam in de handel brengt, al dan niet tegen betaling”. Oftewel als een als importeur of distributeur zijnde haar eigen naam of de naam van haar merk/bedrijf gebruikt, terwijl een product voor de eerste keer in handel wordt gebracht op de Europese markt valt het onder de definitie van een fabrikant.

Voor het tweede element, die een ingrijpende wijziging uitvoert aan het product, komt ook terug bij een artikel 16 CRA. Een andere natuurlijke of rechtspersoon dan de fabrikant, de importeur of de distributeur die een ingrijpende wijziging uitvoert aan het product met digitale elementen, wordt voor de toepassing van deze verordening als fabrikant beschouwd.

Zie in dit licht de definitie distributeur: “…..zonder de eigenschappen hiervan te beïnvloeden.”[86]

Hiermee maakt de wetgever een verschil tussen het enkel verspreiden van een product op de Europese markt en het en het functioneel aanpassen van een dergelijk product met ingrijpende wijzigingen.

Een voorbeeld ter verduidelijking wat het Europese parlement zelf gaf luidt als volgt:

“Het opknappen, onderhouden en repareren van een product met digitale elementen wordt niet beschouwd als ingrijpende wijzigingen, zolang het beoogde gebruik en de functionaliteiten onveranderd blijven en het risiconiveau niet wordt beïnvloed. Echter, als er functionele upgrades worden uitgevoerd tijdens deze activiteiten, kan er wel sprake zijn van een ingrijpende verandering.”

81 Artikel 13 lid 9 CRA.
82 Positie van het Europees Parlement over de Cyber Resilience Act overweging 20, aangenomen bij de eerste lezing op 12 maart 2024.
83 Artikel 14 CRA.
84 Burri & Zihlmann 2023.P.B37.
85 Artikel 14 lid 3 jo. 4 CRA.
86 Artikel 3 lid 21 CRA.

Met andere woorden, als gebruikers (zowel natuurlijke als rechtspersonen) zichzelf in een positie plaatsen die vergelijkbaar is met de rol van fabrikant door ingrijpende wijzigingen aan te brengen in een product, kunnen zij worden onderworpen aan individuele fabrikantverplichtingen.[87] In een dergelijk geval is en gebruiker uitsluitend verantwoordelijk voor het deel van het product dat wordt beïnvloed door de ingrijpende wijziging, of, als de ingrijpende wijziging een impact heeft op de cybersecurity van het product met digitale elementen als geheel, voor het gehele product.

3.5 Vermoeden van Conformiteit

Zoals beschreven moeten fabrikanten producten ontwikkelen, produceren & onderhouden overeenkomstig met de essentiële eisen uit Bijlage I voor de gehele levenscyclus van het product. Ook moeten fabrikanten op de voorgeschreven wijze de conformiteit aan deze eisen beoordelen. In dat licht is het aspect vermoeden van conformiteit van belang. Een vermoeden van conformiteit ziet op overlap met geharmoniseerde normen. Het kan zijn dat bepaalde procedures en werkwijze in plaats zijn waarmee al voldaan is aan de essentiële eisen van de CRA Bijlage I. Dan kan de fabrikant spreken van een vermoeden van conformiteit.[88] Dit is dus niet een vorm van letterlijke uitsluiting, maar een optie voor de fabrikant om aan te tonen dat zijn werkwijze al voldoet aan de eisen van de CRA.

3.5.1 Gevolg van vermoeden van een vermoeden van conformiteit

Een vermoeden van conformiteit is belangrijk omdat het, de vereiste om een derde partij te betrekken bij de conformiteitsbeoordelingsprocedure tenietdoet. Dit geldt voornamelijk voor kritieke producten in klasse 1 met de uitzondering van de kritieke producten uit klasse II, welke altijd een derde partij moeten inschakelen.[89]

Dit is in het bijzonder relevant voor het mkb, gezien het de administratieve druk verlicht. Er hoeft geen eigen documentatie op gesteld te worden om aan te tonen dat aan de essentiële eisen is voldaan; in plaats daarvan kan worden verwezen naar de geharmoniseerde norm. Dit versnelt het proces en vergemakkelijkt de naleving van regelgeving.

Tevens zou de financieel druk die voortvloeit uit een dergelijke beoordeling door een derde ook zwaar zijn voor het mkb. Deze mogen immers enkel gedaan worden door aangemelde instanties die geaccordeerd zijn.[90]

Voordat men kan spreken over een vermoeden van conformiteit moet er dus sprake zijn van een geharmoniseerde norm die voldoet aan de vereisten van de CRA. Een geharmoniseerde norm is een Europese norm die op verzoek van de Commissie is vastgesteld met het oog op de toepassing van harmonisatiewetgeving van de Unie.[91] De commissie zal in samenwerking met ENISA, in het kader van het mkb, zichzelf nog nader inzetten om te zorgen voor dergelijke algemene standaarden. Dit middels een combinatie van bekende normen of via nieuwe standaard compliance processen. Zo hebben zij gesteld Indien er geen geharmoniseerde normen worden vastgesteld of wanneer de geharmoniseerde normen onvoldoende betrekking hebben op de essentiële eisen van deze verordening, moet de Commissie door middel van uitvoeringshandelingen gemeenschappelijke specificaties kunnen vaststellen.[92] Zie tevens ook overweging 39 Verordening (EU) 2019/881 ENISA zal advies geven inzake *guidlines* en *best-practices* voor het conformiteitsproces en daarmee aangeven wanneer men spreekt van een vermoeden van conformiteit. Dit is eigenlijk de uitgebreide toepassing van het normalisatie verzoek die de Commissie heeft gedaan in het kader van deze verordening om een algemeen kader te krijgen voor vermoeden van conformiteit.

Vele producten die kritiek zijn geclassificeerd als kritieke producten zullen waarschijnlijk vallen onder dergelijke standaarden. Deze producten zijn immers voor een reden kritiek, waarmee het logisch is dat er al stappen zijn genomen inzake cybersecurity. Bijvoorbeeld Kritieke producten met digitale elementen die worden uiteengezet in de Bijlage bij deze verordening, maken vanwege hun kritieke karakter al veelvuldig gebruik van verschillende vormen van certificering. Vele vallen dan ook onder de *European Common Criteria-based cybersecurity certification scheme*[93] *(EUCC).*

3.5.2 Geharmoniseerde normen

ENISA heeft onderzoek gedaan naar harmonisatie en standaarden.[94] Om de aanneming van de bepalingen van de CRA te vergemakkelijken, moeten de vereisten zoals bedoeld in Bijlage I CRA worden omgezet in de vorm van geharmoniseerde normen waaraan fabrikanten kunnen voldoen. Ter ondersteuning van de standaardisatie- inspanningen van de EU, probeert het rapport van ENISA de meest relevante bestaande cybersecuritynormen te identificeren voor elk CRA-vereiste. Tevens analyseert het de reeds geboden dekking voor de beoogde reikwijdte van het vereiste en benadrukt het rapport mogelijke *gaps* die moeten worden aangepakt.

Over het algemeen dekken de bestaande normen ten minste gedeeltelijk alle CRA-vereisten. Dit biedt een sterke basis om op voort te bouwen, rekening houdend met de geïdentificeerde gaps. Desalniettemin zijn er geen standaarden gevonden die alle vereisten kan vervullen die zijn opgenomen in de twee afdelingen in Bijlage I van de CRA.

Een complete uitsluiting op basis van eerdere in de markt bekende norm is dus niet mogelijk. De belangrijkste herkende normen uit het rapport zijn: voor afdeling 1

- *ETSI EN 303 645*, in beginsel is hiermee aan alle eisen van Bijlage I afdeling 1 voldaan, alleen spreekt ENISA van enige *gaps* inzake concreetheid.
- *EN ISO/IEC 27002* is ook een belangrijke bouwsteen, hiermee wordt ook al voldaan aan 6 van de 13 essentiële eisen

87 Burri & Zihlmann 2023.P.B23.
88 Artikel 18 CRA.
89 Zie hoofdstuk 3.6 voor meer informatie.
90 Overweging 48 jo. hoofdstuk IV.
91 Artikel 2 lid 1 sub c Verordening (EU) nr. 1025/2012;
92 Overweging 41 jo. artikel 19 CRA.
93 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024. Overweging 46.
94 Ramos E.A. 2024.

Wat betreft Bijlage 1 afdeling 2 is *EN ISO/IEC 30111* het meest relevant, waarmee 5 van 8 eisen inzake respons voldaan.

Men kan dus niet spreken van een vermoeden van conformiteit op basis van deze normen en de *gaps* moeten eerst worden ingevuld tijdens de conformiteitsbeoordelingsprocedure. Of men zal moeten wachten tot de voornoemde normalisatie verzoeken van de EU zijn voldaan, waarmee er dus wel een geharmoniseerde norm komt voor alle vereisten van de CRA.

Voor de herkende overlappingen uit het rapport zie Productie 6[95], het kan dus mogelijk zijn dat er sprake is van een vermoeden van conformiteit als de herkende *gaps* van het rapport al zijn ingevuld.

3.6 Procedures

Zoals reeds vermeld kent de CRA ook een voorgeschreven wijze voor het uitvoeren van de conformiteitsbeoordelingsprocedures.[96] De keuze van een fabrikant voor een conformiteitsbeoordelingsprocedure zoals uiteengezet in Bijlage VI van de CRA, hangt af van de risicoclassificatie van zijn product. Voor niet-kritieke producten kunnen fabrikanten een zelfbeoordeling uitvoeren, waarbij zij verklaren dat hun producten voldoen aan de essentiële veiligheidseisen van Bijlage I. Fabrikanten van kritieke producten van klasse I en II moeten echter de conformiteit aantonen via een EU- typeonderzoek of door volledige kwaliteitsborging, waarbij laatstgenoemde een beoordeling door een derde partij omvat. Hoofdstukken III en IV en Bijlage VI bieden uitgebreide richtlijnen voor de conformiteitsbeoordeling, met name met betrekking tot de procedure en de conformiteitsbeoordelingsinstanties welke in hoofdlijnen hier kort zullen worden besproken.[97]

Er zijn 3 belangrijke aspecten bij procedures.

1. Vermoeden van conformiteit
2. De keuze voor conformiteitsbeoordelingsproces van Bijlage IV
3. Het opstellen van de technische documentatie

3.6.1 Vermoeden van conformiteit en keuze

Een vermoeden van conformiteit heeft ten gevolgen dat enkel hoeft te worden verwezen naar de huidige werkwijze waaruit dit vermoeden voortvloeit. Dit kan gedaan worden middels een interne controle op basis van module A ex artikel 24 lid 1 CRA. Is dit vermoeden van conformiteit niet aanwezig zal ex lid 2 van dit artikel module B, C of H CRA gebruikt moeten worden, waarbij een derde partij betrokken wordt. Hier wordt de conformiteit dus beoordeeld door een aangemelde instantie bij de EU.

Er wordt geschat dat 90% van de producten niet onder kritieke producten vallen.[98] Het staat de fabrikanten van dergelijke producten vrij een interne controle op basis van module A doen van haar producten. Ze kunnen hiermee dus zelf kiezen hoe zij het proces inrichten. In principe hoeft de fabrikant enkel verantwoordelijkheid te nemen voor haar producten door te stellen dat haar product aan alle essentiële eisen van Bijlage I voldoet. De andere 10% zijn producten opgenomen in Bijlage III van de CRA en hebben strengere regels inzake de beoordelingsprocedure. Is het product met digitale elementen opgenomen in klasse 1 van Bijlage III dan is een zwaardere procedure verplicht[99] zo stelt de Commissie:

> *"Er is aanvullende zekerheid vereist om conformiteit aan te tonen met de essentiële eisen die zijn vastgesteld in deze Verordening. De fabrikant moet geharmoniseerde normen, gemeenschappelijke specificaties of Europese certificeringsschema's voor cyberbeveiliging toepassen die zijn aangenomen krachtens Verordening (EU) 2019/881 als hij de conformiteitsbeoordeling onder zijn eigen verantwoordelijkheid wil uitvoeren (module A). Als de fabrikant dergelijke geharmoniseerde normen, gemeenschappelijke specificaties of Europese certificeringsschema's voor cyberbeveiliging niet toepast, moet de fabrikant een conformiteitsbeoordeling ondergaan met betrokkenheid van een derde partij (op basis van Modules B en C of H)."*[100]

Dit betekent dat een fabrikant van kritieke producten in klasse 1 enkel een interne controle mag doen, indien zij gebruik heeft gemaakt van in de markt bekende standaarden. In een dergelijk geval kunnen we immers spreken van de reeds beschreven vermoeden van conformiteit.

Echter zoals reeds beschreven bestaan er nog geen cybersecurity standaarden die volledig voldoen aan de CRA, een interne beoordeling op basis van module A voor kritieke producten is nu in principe dus nog niet mogelijk.

Gezien het grotere cybersecurity-risico verbonden aan het gebruik van kritieke producten met digitale elementen die vallen onder klasse II, moet de conformiteitsbeoordeling altijd een derde partij omvatten, zelfs als het product volledig of gedeeltelijk voldoet aan geharmoniseerde normen, gemeenschappelijke specificaties of Europese certificeringsschema's voor cyberbeveiliging.

Is het product met digitale element opgenomen in klasse 2 van Bijlage III, betekent dit dat zelfs als de fabrikant kan spreken van een vermoeden van conformiteit op basis van eerdere normen en standaarden, er alsnog een derde partij moet worden ingeschakeld bij de procedure.[101] Dit is dus een hele ingrijpende procedure van de CRA en daarom ook alleen toepasbaar op de meest risicovolle producten.

3.6.2 Documentatie

Tot slot is het een verplichting voor de fabrikant om technische documentatie op te stellen zoals uitgebreid vastgesteld in Bijlage II van de CRA. De risicobeoordeling moet worden

95 Ramos E.A. 2024.
96 Zie hoofdstuk 3.4.
97 Burri & Zihlmann 2023. P.B33.
98 TIC Council, https://www.tic-council.org/news-and-events/news/press-release-tic-council-welcomes- european-commissions-proposal-cyber-resilience-act, September 2022.
99 Artikel 24 lid 2 CRA.
100 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024.
101 Artikel 24 lid 3 CRA.

opgenomen in de technische documentatie zoals uiteengezet in artikel 23 en Bijlage V. Bovendien moeten de gekozen conformiteitsbeoordelingsprocedure en -verklaring worden opgenomen.

Fabrikanten hebben ook verschillende documentatieverplichtingen met betrekking tot het omgaan met kwetsbaarheden en informatie verstrekt door derden. In het bijzonder specificeert artikel 23 CRA de inhoud van de technische documentatie die door de fabrikant moet worden opgesteld voordat het product op de markt wordt gebracht en die gedurende tien jaar na het op de markt brengen van het product ter beschikking moet worden gehouden van de markttoezichtautoriteiten.[102] Hier staan ook de procedures voor het verstrekken van deze documentaties beschreven.

3.7 Het mkb

3.7.1 Definitie en plannen

Gezien deze zwaarwegende administratieve en financiële lasten die beoordelingsprocessen zullen opleggen aan de fabrikanten, naast de al aanzienlijke inspanningen om te voldoen aan de essentiële eisen tijdens de ontwerp, ontwikkelings- en productiefasen van het product, komt de wetgever hun enigszins tegemoet. Met name heeft de Commissie gekeken naar het mkb en startups met deze tegemoetkoming. De definitie gehanteerd in Europese wetgeving is:[103] Tot de categorie kleine, middelgrote en micro-ondernemingen behoren ondernemingen waar minder dan 250 personen werkzaam zijn en waarvan de jaaromzet 50 miljoen EUR of het jaarlijkse balanstotaal 43 miljoen EUR niet overschrijdt.

De Commissie heeft veel toezeggingen gedaan m.b.t. wat zij beoogd te doen voor het mkb om de compliance van de verordening te bevorderen. Dit ziet op financiële tegemoetkomingen, kennisdeling, opstellen van richtlijnen en de reeds aangestipte standaarden en normalisatie verzoeken.[104] De belangrijkste hiervan is dan ook het besproken eerder besproken ENISA-rapport waar een geharmoniseerde standaard uit zal voortvloeien.[105] Aangezien de verordening nog niet definitief is, zijn ook de concrete plannen van de Commissie nog niet vastgesteld. Daarom is het ook niet mogelijk om een uitgebreid overzicht te bieden wat en hoe het mkb het best kan profiteren. Wel volgt hierna een korte opsomming van wat het mkb kan verwachten, waarom dit voordelen voor hen zijn en wat deze inhouden.

3.7.2 Voordelen

- **Begeleiding van de Commissie**
  De Commissie zal economische operatoren begeleiden, met name micro-ondernemingen en kleine en middelgrote ondernemingen, te helpen bij de toepassing van de verordening. Deze begeleiding zal onder meer de reikwijdte van de verordening omvatten, met speciale aandacht voor externe gegevensverwerking en de implicaties daarvan voor ontwikkelaars van vrije en open-source software, evenals criteria voor ondersteuningsperiodes voor producten met digitale elementen, de interactie tussen de verordening en ander EU-recht en wat als ingrijpende wijziging wordt gezien in het oog van de bijzonder gevallen voor importeurs en distributeurs.[106] Deze begeleiding is zowel formeel in de vorm van amendementen aan de verordening, uitvoeringsbesluiten als informeel in de vorm van hulpmiddelen, trainingen etc.[107]

- **Training en vaardigheidsontwikkeling:**
  De Commissie zal zorgen voor trainingen en vaardigheidsontwikkeling met betrekking tot compliance met de verordening.[108] Denk hierbij aan gepubliceerde onderzoeken, standaard modellen en die de Commissie aanbiedt over de CRA.

- **Vereenvoudigde technische documentatie**
  De Commissie zal standaarden vaststellen voor de technische documentatie[109] in een vereenvoudigde versie voor het mkb. Bedrijven kunnen er echter ook voor kiezen om de uitgebreide formulieren van de Commissie te gebruiken.[110] Op deze manier hoeven fabrikanten niet zelf technische documentatie op te stellen, maar kunnen zij gebruik maken van een standaard format.

- **Regulatory sandboxes**
  Deze bieden een experimentele ruimte waarin nieuwe technologieën, innovatieve producten, diensten of bedrijfsmodellen kunnen worden getest onder een gecontroleerd regelgevend kader. Dit stelt bedrijven in staat nieuwe ideeën te ontwikkelen en te implementeren zonder onmiddellijk aan alle processen en eisen van de CRA te hoeven voldoen.[111]

- **Lagere kosten voor mkb**
  Aangemelde instanties zullen rekening houden met de specifieke belangen en behoeften van kleine en middelgrote ondernemingen bij het vaststellen van vergoedingen voor conformiteitsbeoordelingsprocedures, waarbij deze kosten worden verlaagd in verhouding tot hun specifieke belangen en behoeften.[112] Dit leidt ertoe dat de kosten voor een verzwaarde procedure door een derde minder ingrijpend zijn voor het mkb.

102 Chiara, International Cybersecurity Law Review 2022/3. P.261.
103 Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro- ondernemingen 2003/361/EC.
104 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024.
105 Zie hoofdstuk 3.5.
106 Zie hoofdstuk 3.4.4.
107 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024. Overweging 6.
108 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024. Overweging 23.
109 De technische documentatie als bedoeld in productie 5.
110 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024. Overweging 94.
111 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024. Overweging 98.
112 Artikel 14 lid 5 CRA.

- **Standaardisatieprocessen**
  De laatste en belangrijkste geïdentificeerde voordelen zijn de standaardisatieprocessen.[113] De Commissie zal namelijk standaardisatieprocessen opzetten waarbij sprake kan zijn van een vermoeden van conformiteit. De ontwikkeling van deze standaarden zal tijdig worden uitgevoerd, zodat producten die via module A- beoordelingen via de interne controleprocedure snel kunnen worden goedgekeurd zonder vertragingen.[114] Dit heeft het gevolg dat mkb onderneming niet zelf processen en documenten hoeven op te stellen, maar enkel hoeven te voldoen aan de standaarden van de EU.

3.8 Beantwoording Theorie deelvragen

Hier worden kort de ontwerpeisen besproken op basis de theoriedeelvragen zoals gedefinieerd in hoofdstuk 1, aan de hand van het theoretisch onderzoek. Voor meer informatie over de eisen wordt dan ook verwezen naar het theoretische kader.

Welke ontwerpeisen vloeien voort uit parlementaire stukken m.b.t. de inhoud van de beslisboom?

- Duidelijkheid over de voordelen voor het mkb die er aan zullen komen, zoals geïdentificeerd in parlementaire stukken. Omdat dit onderzoek in het kader van het project CSNN gefocust is op het mkb, is het een eis voor de beslisboom om het mkb te herinneren aan aankomende opties die het makkelijker maakt voor hen om aan de CRA te voldoen.

Welke ontwerpeisen voor de beslisboom vloeien voort uit de toepasselijke wetsartikelen en bijlages uit de CRA, de herziene NIS2 en (juridische) vakliteratuur m.b.t. de inhoud van de beslisboom?

Het belangrijkste aspect dat voortvloeit uit deze deelvraag zijn de stappen die moeten worden uitgewerkt in de beslisboom. De volgende stappen zijn in de theorie herkent en dienen dus als eis te worden opgenomen in de beslisboom:

1. Valt het onder de scope van de CRA?[115]
   a. Materiële scope, is het een product met digitale elementen, ook wel Internet of Things producten
   b. Is er sprake van een Fabrikant, importeur of distributeur
2. Is er sprake van een letterlijke uitsluiting?[116]
   a. Op basis van het type product/service (zoals SaaS of Opensource Software)
   b. Op basis van een overlappende verordening
3. In welke risicoklasse valt het product?[117]
   a. Standaardcategorie
   b. Kritieke lijst
      i. Klasse 1
      ii. Klasse 2
4. Is er sprake van een vermoeden van conformiteit?[118]
5. Conclusie, met meer informatie en uitleg over de gevolgen.

Dit betekent dat de volgende aspecten als moeten behandeld worden in deze stappen:

- Onderscheiding van uitgesloten producten op basis van het toepassingsgebied van de CRA.
- De verschillen tussen fabrikanten, importeurs en distributeurs moeten worden benadrukt zoals gedefinieerd in hoofdstuk II van de CRA.
- Verduidelijking van de verplichtingen uit de CRA.
- Beschrijving van de procedures, met bijzondere nadruk op de conformiteitsbeoordelingsprocedure.
- Behandeling van het vermoeden van conformiteit en de daaruit voortvloeiende gevolgen, zoals beschreven in hoofdstuk III van de CRA.

113 Positie van het Europees Parlement over de Cyber Resilience Act, aangenomen bij de eerste lezing op 12 maart 2024. Overweging 80 jo. 81.
114 Zie hoofdstuk 3.5 jo. 3.6.
115 Zie hoofdstuk 3.2.
116 Zie hoofdstuk 3.3.
117 Zie hoofdstuk 3.4.1.
118 Zie hoofdstuk 3.5.

4. Ontwerpeisen vanuit de praktijk

In dit hoofdstuk worden de praktijkdeelvragen beantwoord aan de hand van de uitkomsten van de afgenomen interviews en de test van de beslisboom. Er wordt antwoord gegeven op de volgende deelvragen:

- Welke ontwerpeisen voor de beslisboom vloeien voort uit eerdere ervaring met het implementeren van Europese wetgeving door mkb-ondernemers m.b.t. de inhoud van de beslisboom?
- Welke ontwerpeisen voor de beslisboom vloeien voort uit een analyse van de huidige werkwijze van de ondernemers inzake cybersecurity m.b.t. de inhoud van de beslisboom?
- Welke ontwerpeisen voor de beslisboom zijn af te leiden uit een test van een concept van de beslisboom bij mkb-ondernemers?

4.1 Interviews

Om de deelvragen te beantwoorden, zijn er interviews afgelegd met verschillende mkb-ondernemers die onder de scope van de CRA vallen. Deze interviews zijn specifiek gefocust op ondernemers die een interessant draagvlak hebben op basis van de onderzochte aspecten uit de theorie. Zo kan worden vergeleken hoe theoretische uitzondering en bijzonder gevallen zich vertalen in de praktijk. Met als doel om op basis van deze vergelijking ontwerpeisen voor de beslisboom te identificeren.

Deze theoretisch interessante aspecten zijn:

- De SaaS uitzondering[119], de artikel 15 jo. 16 bijzondere gevallen waar een distributeur als een fabrikant wordt aangemerkt[120] en de nationale veiligheid uitzondering[121] welke in de praktijk onderzocht bij de onderneming Onderneming A.

119 Zie hoofdstuk 3.3.5.
120 Zie hoofdstuk 3.4.4.
121 Zie hoofdstuk 3.3.1.

- Een vermoeden van conformiteit of complete uitsluiting op basis van een overlappende verordening[122] en Software als een product met digitale elementen is in de praktijk onderzocht bij de onderneming Onderneming B.
- Tot slot is er nog gekeken naar een complete uitsluiting op basis van een overlappende verordening[123] bij de onderneming Onderneming C.

4.1.1 Onderneming A

Onderneming A is een onderneming die zich richt op het monitoren van deformatie in de bouwsector. Het bedrijf koopt sensoren in die ze aan hun klanten leveren. Naast de sensoren leveren ze ook zelf ontwikkelde hardware en software aan klanten in Europa en Noord-Amerika. De sensoren van Onderneming A zijn uitgerust met een dynamische *gateway* die verbinding maakt met een database, waardoor gebruikers via internet *on demand* toegang hebben tot de gegevens die de sensoren lezen.

Om deze data toegankelijk te maken, biedt Onderneming A een *Application Programming Interface*[124] (hierna: "API") aan, wat een oplossing is voor externe gegevensverwerking.[125] Dit betekent dat de producten en diensten van Onderneming A, inclusief de software- en hardwarecomponenten, vallen onder de CRA. De CRA is van toepassing op alle producten met digitale elementen, en omdat Onderneming A zowel software als hardware levert die essentieel zijn voor de verwerking en toegankelijkheid van gegevens, zijn zij een expliciet voorbeeld van het materiële toepassingsgebied van de CRA.

Huidige situatie

Onderneming A richt zich momenteel op de beveiliging van hun producten door middel van verschillende technieken. De sensoren die ze gebruiken bevatten encryptiesoftware die data verstuurt naar een gelicentieerde database, welke wordt beveiligd door de ontwikkelaar van de servers. In sommige bijzondere gevallen maken ze ter plaatse een lokale server, zonder externe gegevensverwerking. Hoewel dit uitzonderlijk is en volgens de oprichter zelden voorkomt, is deze manier van werken als de meest veilige optie. Deze lokale aanpak maken de sensoren uitgesloten van de CRA, immers is een dergelijk product dan geen oplossing meer voor externe gegevensverweking.[126]

Onderneming A beveiligt hun producten niet specifiek op basis van wetgeving of normen. Soms vereisen overheid instanties, zoals die op aanbestedingsplatformen, een minimale beveiliging volgens ISO-normen, zoals 9001 certificering. Dit is echter afhankelijk van de opdracht en het betreffende bedrijf of organisatie. De ervaring van Onderneming A met wetgeving is daarom ook beperkt. Ze hebben nog niet vaak te maken gehad met wetgevingsvereisten zoals de AVG, die voor hen niet relevant is. Het bedrijf doet het minimale wat van hen benodigd is om te voldoen aan wettelijke eisen. Ze zijn zich bewust van mogelijke

122 Zie hoofdstuk 3.3.3.
123 Zie hoofdstuk 3.3.1.
124 Een API is een computerprogramma dat gegevens/data kan lezen en vertalen naar een interface, om deze vervolgens te presenteren.
125 Zie hoofdstuk 3.2.1 oplossingen voor gegevensverwerking op afstand.
126 Zie hoofdstuk 3.2.1.

toekomstige regelgeving, zoals de *Data Governance Act* (Hierna: "DGA"), maar hebben nog geen beleid of specifieke maatregelen genomen met betrekking tot wetgeving omdat ze een mkb-bedrijf zijn en enkel voldoende willen doen om op de markt te kunnen blijven opereren.

Onderneming A is daarom wel benieuwd hoe bezwarend de CRA zal zijn en wat ze allemaal moeten doen om te voldoen aan deze nieuwe wetgeving. Ze zijn vooral geïnteresseerd in de praktische implicaties en de mate van inspanning die van hen verwacht wordt om aan de CRA te voldoen.

Distributeur

Zoals reeds vermeld is het doel van het interview om interessante aspecten uit de theorie in de praktijk te vergelijken met de werkwijze van de praktijk. In dit geval komen de bijzondere gevallen waar een distributeur als een fabrikant wordt aangemerkt aan bod. Zoals beschreven is dit het geval wanneer een importeur/distributeur een product op de markt brengt onder haar eigen merknaam, of als zij het product zodanig aanpassen met ingrijpende wijzigingen, dat dit invloed heeft op het risiconiveau c.q. de functionaliteit van het product.[127] Deze aspecten worden dus aan de hand van de werkwijze van Onderneming A als een Distributeur vergeleken.

Onderneming A gaf aan dat het heel gebruikelijk is om producten op de markt brengen onder hun eigen merknaam. Daarnaast kunnen bedrijven meerdere economische rollen innemen. Zo kan een bedrijf als fabrikant handelen bij het maken van een API, maar als distributeur optreden bij het leveren van software en het presenteren van data. Dit gebeurt allemaal bij Onderneming A.

Het is echter niet gebruikelijk dat Onderneming A producten die zij inkopen zodanig wijzigt of verwerkt dat dit invloed heeft op de digitale elementen of de beveiliging van het product. Zij beginnen hier pas mee bij aanbestedingen als het een verplichting is of als de wet hen daartoe verplicht. De fabrikant maakt het product en schrijft ook voor hoe het werkt en hoe het product het beste beveiligd kan worden. Vaak gebeurt dit in opdracht of in samenwerking met de leverancier. Bijvoorbeeld, een *Pull API* kan samen met de leverancier worden gemaakt voor alle data die de sensoren verzamelen. Met deze *Pull API* kan alle data van de fabrikant op een centrale eigen server worden opgeslagen, en deze servers worden beveiligd volgens de geldende licenties. Op deze manier neemt Onderneming A nooit de rol van de fabrikant over.

Uit de werkwijze van Onderneming A blijkt dat distributeurs vaak als fabrikanten worden aangemerkt omdat ze producten onder hun eigen merknaam op de markt brengen. Het komt echter vrijwel nooit voor dat producten zodanig worden aangepast dat dit invloed heeft op de cybersecurity van het product, omdat de voorgeschreven werkwijzen van de fabrikant worden gevolgd.

Een ander veelvoorkomend geval is dat een bedrijf dat hoofdzakelijk als distributeur handelt (zoals het inkopen van sensoren en deze aanbieden) ook als fabrikant optreedt met nevenactiviteiten, zoals het zelf ontwikkelen van software voor de presentatie van data. Deze

127 Zie hoofdstuk 3.4.4 voor meer informatie.

combinatie van rollen benadrukt de complexiteit van de huidige markt en de noodzaak voor duidelijke uitvoeringsbesluiten en andere vormen van toelichting over de CRA.[128]

Uitsluitingen
Onderneming A biedt Software as a Service (SaaS) aan in de vorm van toegang tot hun *API*, waarmee klanten de data kunnen inzien. De SaaS die zij ter beschikking stellen, geeft klanten de mogelijkheid om via een unieke gebruikersnaam en wachtwoord altijd de data via hun platform te bekijken.

Voor kleine klanten is het noodzakelijk om de SaaS van Onderneming A te gebruiken in combinatie met de sensoren, terwijl grote klanten die over een eigen platform beschikken, de software als dienst niet nodig zijn. Zij kunnen de hardware van Onderneming A verbinden met hun eigen systemen. Dit leidt ertoe dat de CRA soms wel en soms niet van toepassing is, afhankelijk van de manier waarop de diensten van Onderneming A worden gebruikt. Als klanten de SaaS gebruiken kan dit uitgesloten zijn op basis van de definitie van SaaS. Als klanten echter alleen de hardware gebruiken en de data zelf beheren, valt dit wel onder de CRA. Onderneming A geeft aan dat dit gebruikelijk is voor dergelijke leveranciers van sensoren.

De uitzondering voor nationale veiligheid is een heel andere situatie en is zeer ongebruikelijk voor Onderneming A. Hoewel hun sensoren worden gebruikt om de veiligheid van publieke gebouwen en bruggen te monitoren, is het primaire doel meestal niet specifiek gerelateerd aan nationale veiligheid. De sensoren hebben meestal een ander doeleinde. Onderneming A geeft aan dat zij zich moeilijk kunnen voorstellen dat deze uitzondering in de praktijk vaak voorkomt voor mkb-ondernemers. Nationale veiligheid is een zeer specifieke en uitzonderlijke categorie.

4.1.2 Onderneming B
Onderneming B ontwikkelt AI-software voor oplossingen met betrekking tot de overbelasting van het stroomnet. Ze bouwen algoritmes die data aggregeren en de disbalans van het net verhelpen.[129] Hun werk omvat het ontwikkelen van software voor *machine learning*-algoritmes en het bouwen van *API-interfaces* voor het systeem. Onderneming B levert geen applicaties of controlesystemen, maar richt zich enkel op de backend software en AI-systemen.

Dit is een klassiek voorbeeld van software wat valt onder de definitie van producten met digitale elementen. Hun software integreert andere systemen en het stroomnet, dit maakt het een oplossingen voor gegevensverwerking.[130] Onderneming B werkt voornamelijk in opdracht van VattenFall. Ze zijn een Klimaat-Tech startup en zijn niet zelfstandig actief op de markt, maar opereren via samenwerkingen en opdrachten voor het netbeheer. Aangezien Onderneming B AI-systemen en *backend software* ontwikkelt in opdracht van een actieve marktdeelnemer, valt hun werk onder de CRA. Er dient wel gekeken te worden naar de overlap met de AI verordening.

128 Zoals uit hoofdstuk 3.7 blijkt zal de Commissie hier ook nog nader over uiten.
129 Het aggregeren van data en oplossen van disbalans op stroomnetwerk betekent dat de algoritmes data verzamelen en aan de hand van die data bepalen hoe de balans van het stroomnetwerk geoptimaliseerd kan worden.
130 Zie hoofdstuk 3.2.1.

Huidig situatie
Onderneming B ontwikkelt hun systemen in overleg met Vattenfall, waarbij ze rekening houden met de Algemene Verordening Gegevensbescherming (AVG). Ze werken ook samen met Vattenfall om ervoor te zorgen dat hun dataverwerkingsbeleid aan alle eisen voldoet. Hun werk aan cybersecurity is nog in ontwikkeling, vooral gericht op de *back-end* van hun systemen. Onderneming B erkent dat ze mensen moeten aannemen om hun kennis op dit gebied te versterken, aangezien ze momenteel weinig expertise in huis hebben wat gebruikelijk is voor startups.

De focus van Onderneming B ligt voornamelijk op de ontwikkeling van hun software. Als startup stellen ze dat zaken zoals compliance vaak later aan bod komen. Omdat ze nog niet zelfstandig op de markt actief zijn, doen ze alleen het minimale dat vereist is. Op dit moment conformeren ze zich aan OWASP standaard level 1, wat ook van hen wordt verwacht.[131]

Op de vraag of er beleidsstukken of richtlijnen zijn betreffende hun cybersecuritypraktijken, geeft Onderneming B aan dat dit bij mkb-bedrijven en vooral bij startups die nog niet op de markt zijn, ongebruikelijk is. Dit benadrukt de uitdaging van dit onderzoek, omdat jonge bedrijven niet vanaf het begin aan alle compliance- eisen kunnen voldoen, terwijl ze hun producten en diensten nog ontwikkelen en verfijnen.

AI verordening
Onderneming B is niet bekend met de AI-verordening en geeft aan dat de meeste bedrijven in hun markt nog niet voorbereid zijn op deze wetgeving. Ze willen graag weten of hun huidige algoritmes voldoen aan de vereisten en wat de overlap is met de CRA. Echter voldoen ze enkel aan minimale eisen, zoals overeengekomen met Vattenfall, namelijk OWASP level 1.[132]

Onderneming B benadrukt tevens dat de ontwikkeling van AI sneller gaat dan de wetgeving. Dit betekent dat de markt nog niet klaar is voor de vereisten van de nieuwe AI verordening. Er is een duidelijk gebrek aan kennis en voorbereiding in de markt met betrekking tot zowel de CRA als de AI verordening. Het feit dat bedrijven niet klaar zijn voor de vereisten van de nieuwe AI verordening is opmerkelijk te noemen, omdat bedrijven zijn uitgesloten van de CRA als ze voldoen aan de vereisten en procedures van de AI-verordening.

4.1.3 Onderneming C
Onderneming C is een bedrijf dat drones maakt en innoveert in dit veld. Ze zijn actief in het monitoren van industrieterreinen, beveiliging en het transport van medische hulpmiddelen met hun drones. Dergelijke producten vallen onder de CRA, omdat de drones digitale elementen bevatten en voor hun besturing een externe verbinding nodig hebben. De drones worden alleen al gereguleerd in sectorale wetgeving en zijn dus uitgesloten van de CRA.[133] Ze zijn echter ook

131 De OWASP standaarden zijn niet behandeld in hoofdstuk 3.5, omdat deze voornamelijk zien op informatie systemen (in dit geval AI-training). Dergelijke systemen worden wel behandeld in de AI verordening.
132 Zoals beschreven in hoofdstuk 3.5.2 voldoen geen enkele normen (ook de niet aanwezige normen in het ENISA rapport) aan alle vereisten.
133 Zie hoofdstuk 3.3.1 luchtvaartverordening.

actief in het testen van regelgeving binnen hun vakgebied, waardoor eerdere ervaring op dit gebied kunnen worden vergeleken met de mogelijkheid voor de CRA.

De ervaring van Onderneming C met sectorale regelgeving en de vereisten voor drones toont aan dat innoveren binnen deze vereisten uitdagend is. Het bedrijf probeert via Europese initiatieven zoals *regulatory sandboxes* een omgeving te creëren waarin ze kunnen innoveren zonder belemmeringen door regelgeving. Ze denken dat dit concept ook goed zou kunnen aansluiten bij de CRA. Echter heeft Onderneming C gemerkt dat testomgevingen rondom de luchtvaartverordening en drone regelgeving geleerd dat het opzetten van dergelijke *sandboxes* voor mkb-bedrijven zeer moeilijk is. Dit maakt hen benieuwd naar de specifieke vereisten van de CRA en hoe deze zich verhouden tot de luchtvaartverordening. Hoewel de EU heeft aangegeven *regulatory sandboxes* te willen realiseren voor de CRA[134], wijst de ervaring van Onderneming C erop dat dit een uitdagende optie kan zijn voor mkb-bedrijven.

4.2 Analyse van de interviews

4.2.1 Ontwerpeisen op basis van eerdere ervaringen

Uit de ervaringen rondom wetgeving blijkt dat mkb-ondernemingen vaak het minimale doen om het product op de markt te brengen. Zo stellen de ondernemers:

- *Ervaring van Onderneming B rondom AVG*, Onderneming B geeft aan dat bij mkb-bedrijven en vooral bij startups die nog niet op de markt zijn, het ongebruikelijk is om beleid of aandacht te besteden aan extra eisen. Dit benadrukt de uitdaging van dit onderzoek, omdat jonge bedrijven niet vanaf het begin aan alle compliance-eisen kunnen voldoen, terwijl ze hun producten en diensten nog ontwikkelen en verfijnen.
- *Ervaring Onderneming A rondom regelgeving*, ze hebben nog geen beleid of specifieke maatregelen genomen met betrekking tot wetgeving omdat ze een mkb-bedrijf zijn en enkel voldoende willen doen om op de markt te kunnen blijven opereren.

Hieruit blijkt dat de beslisboom moet tonen wat de minimale vereisten zijn van de CRA en wat benodigd is om een product op de markt te brengen. Dit zijn de essentiële eisen van Bijlage I en de technische documentatie van Bijlage II CRA. De beslisboom dient deze dus in hoofdlijnen te presenteren op een overzichtelijke manier. Bijvoorbeeld aan de hand van het samenvatten van deze bijlages in een tabel, welke in de interactieve boom zijn verwerk bij de desbetreffende stappen.[135]

Uit de ervaring van Onderneming C blijkt dat het realiseren van een *regulatory sandbox* lastig is voor het mkb. Dit onderzoek is gericht op het mkb en de beslisboom dient dan ook de beste voordelen voor het mkb te presenteren. Er moet daarom gekeken te worden naar de meest relevante opties van de, door de Commissie voorgestelde, voordelen voor het mkb.[136]

134 Zie hoofdstuk 3.7.
135 Zie productie 8.
136 Zie hoofdstuk 3.7.

4.2.3 Ontwerpeisen op basis van huidige werkwijze

De werkwijze van Onderneming A laat zien dat de toepassing van de CRA complex en situationeel afhankelijk kan zijn. Onderneming A gaf aan dat het heel gebruikelijk is om producten op de markt brengen onder hun eigen merknaam. Wat zou leiden tot het innemen van de rol van een fabrikant.[137] Daarnaast kunnen bedrijven meerdere economische rollen innemen. Zo kan een bedrijf als fabrikant handelen bij het maken van een API, maar als distributeur optreden bij het leveren van software en het presenteren van data. Dit gebeurt allemaal bij Onderneming A en zij gaven tevens aan dit gebruikelijk is. Het is voor de beslisboom daarom een ontwerpeis om te kijken naar een specifiek product. Over het algemeen kunnen er bij meerde producten verschillende rollen worden ingenomen en voor verschillende producten ook andere situaties van toepassing zijn.

Onderneming B merkte op dat AI-ontwikkeling de wetgeving inhaalt, waardoor bedrijven nog niet voorbereid zijn op de AI verordening. Dit gebrek aan kennis en voorbereiding geldt ook voor de CRA, aangezien geen een van de geïnterviewde ondernemers bekend waren met de verordening. Omdat bedrijven uitgesloten zijn van de CRA als ze voldoen aan de AI-verordening, moet de beslisboom duidelijk maken dat een uitzondering op basis van AI systemen onwaarschijnlijk is, aangezien beide verordeningen nog niet in werking zijn. Daarnaast dient de beslisboom duidelijk te maken dat de CRA zelf nog niet in werking is getreden, voordat er ingegaan wordt op de inhoudelijke verplichtingen. Deze vraag kwam namelijk naar voren in alle interviews, door dit aan het begin te behandelen zorgt de beslisboom voor meer duidelijkheid over wat er van de ondernemers wordt verwacht.

Tot slot blijkt uit de huidige situatie dat er in sommige gevallen gebruikt wordt gemaakt van geharmoniseerde normen. Zo geven de ondernemers aan:

- *Onderneming A* Soms vereisen overheid instanties, zoals die op aanbestedingsplatformen, een minimale beveiliging volgens ISO-normen, zoals 9001 certificering. Dit is afhankelijk van de opdracht en het betreffende bedrijf of organisatie.
- *Onderneming B* Wij doen het minimale wat van ons verwacht wordt in overleg met VattenFal. Wij zijn daarom compliant aan de namelijk OWASP level 1.

Beide ondernemingen vroegen af of deze ook afdoende waren voor de verplichtingen van de CRA of, indien niet, er een hogere versie is die wel voldoet hieraan. Het is daarom een eis van de beslisboom om aan te geven dat geen van de huidige normen voldoen aan alle eisen van de CRA, maar dat de Commissie zich wel aan het inspannen is hiervoor met standaardisatie verzoeken.[138]

137 Zie de bijzondere gevallen h3.4.4.
138 Zie hoofdstuk 3.5.2.

4.3 Beroepsproduct test

4.3.1 Opzet en resultaten

Aan de hand van het theoretisch kader en de ontwerpeisen zoals verwoord in hoofdstuk 3.8, is een blauwprint gemaakt voor de beslisboom die de hoofdelijke stappen en ontwerpeisen in kaart brengt. Deze blauwprint is besproken bij de CSNN-bijeenkomst, waar is afgeweken van digitale versie gezien praktische mogelijkheden van het hosten van een dergelijke digitale versie. Daarom is op basis van de blauwprint een eerste concept gemaakt als een analoge versie van de beslisboom.[139] Enkel zoals beschreven in hoofdstuk 1.3 leidde de analoge versie tot veel takken en weinig mogelijkheid om dingen te beschrijven in de Beslisboom. Dit bleek onduidelijk op basis van de test. Alleen een volledig interactieve[140] blijkt niet praktisch voor de opdrachtgever CSNN. Daarom is nog een alternatieve optie voorgesteld via *TypeForum*.[141] Dit is een interactieve optie waarbij dezelfde stappen worden doorlopen.

De test van het beroepsproduct is uitgevoerd met zowel de analoge als de interactieve versie van de beslisboom. Voorafgaand aan de test is vastgesteld welke conclusie de onderneming zou moeten trekken en welke antwoorden op welke vragen gegeven zouden moeten worden. Dit diende als basis voor het evalueren van de werking van de beslisboom. Allereerst werd de analoge versie van de beslisboom besproken met de deelnemers. Er werd gevraagd of zij alle stappen en conclusies begrepen, wat zij eventueel nog wilden toevoegen, en of zij deze versie als bruikbaar ervaarden.

Na de bespreking van de analoge versie, werd de interactieve versie gezamenlijk doorlopen. Hierbij werd stap voor stap gekeken of de juiste keuzes werden gemaakt en of de juiste conclusies werden getrokken. Het doel was om te verifiëren of de interactieve versie effectief in het begeleiden van de gebruiker naar de juiste uitkomst. Tot slot werd opnieuw aan de deelnemers gevraagd of zij alles begrepen hadden, wat zij nog wilden terugzien in de interactieve versie, en of zij deze versie als bruikbaar beschouwden.

Alle geïnterviewde ondernemers kwamen op de juiste conclusies. De bespreking en feedback van de test toonde echter wel punten die aanpassing vereiste. Deze punten zijn opgenomen als ontwerpeisen.

4.3.2 Overige ontwerpeisen

Op basis van de test

Er zijn Linkjes toegevoegd naar betrouwbare bronnen voor meer informatie om de begrijpelijkheid van de genoemde stappen te bevorderen. Deze linkjes zijn vervolgens ook als hyperlinks verwerkt, bijvoorbeeld bij de stap ‘Voldoen de AI-systemen aan de AI verordening?’ Is aan toegevoegd: De AI verordening is net als de CRA nog niet in werking, het is daarmee onwaarschijnlijk dat uw producten aan beide vereisten voldoen.
Bekijk de voortgang van beide verordeningen voor meer informatie:.

139 Zie productie 7.
140 Zie de voorbeelden H1.7.
141 Zie productie 8.

Op basis van de feedback is per stap meer uitleg gegeven over de termen in combinatie met de hyperlinks, omdat werd aangegeven dat het soms moeilijk te begrijpen was. Bijvoorbeeld werd bij de stap ‘Is uw product opgenomen in klasse 1 van de kritieke lijst van de CRA?’ toegevoegd: Over het algemeen wordt een product als kritiek beschouwd als de negatieve impact van het misbruik van mogelijke cybersecuritykwetsbaarheden in het product ernstig kan zijn. De volgende producten zijn genoemd in klasse 1.[142]

Tot slot is pp basis van de feedback van OmniDrone toegevoegd dat, hoewel producten niet op basis van de CRA beveiligd hoeven te zijn, deze wel beveiligingseisen hebben op basis van de uitgesloten regelgeving. Verder gaven de ondernemers aan tevreden te zijn met de beslisboom als beroepsproduct wat zij zagen als een nuttig en overzichtelijk hulpmiddel.

Op basis van het Lectoraat Juridische Aspecten van Ondernemerschap

Zoals beschreven in hoofdstuk 1.4 wenste de opdrachtgever meerdere versies van het beroepsproduct te zien. Op basis hiervan zijn ontwerpeisen gemaakt en aanpassingen doorgevoerd. Naast enkele kleinere opmaak- en vormgevingsaanpassingen, is de mogelijkheid en wens benadrukt om zowel de interactieve als de analoge versie op te leveren en uit te werken.

Inhoudelijk is een disclaimer en een optie om terug te gaan bij de vragen toegevoegd. De analoge versie is daarnaast in A3-formaat gezet voor leesbaarheid en overzichtelijkheid. Deze was eerst enkel als .jpg-bestand geleverd. De QR-code, die oorspronkelijk naar de website van CSNN verwees, is aangepast om te verwijzen naar de interactieve beslisboom, nu beide opties worden aangeleverd.

142 Hier is een kopie van productie 4 toegevoegd.

5. Analyse en conclusie

5.1 Analyse van de Ontwerpeisen

Uit het theorie-onderzoek zijn diverse ontwerpeisen naar voren gekomen voor de beslisboom omtrent de CRA. Deze ontwerpeisen zijn gebaseerd op parlementaire stukken en juridische literatuur, waarin de belangrijkste stappen en verplichtingen voor producten met digitale elementen zijn beschreven. De kernpunten omvatten:

- de materiële scope;
- uitsluitingen;
- verplichtingen van fabrikanten, importeurs en distributeurs;
- en de conformiteitsbeoordelingsprocedures.

In het praktijkonderzoek, bestaande uit interviews en tests met mkb-ondernemers, is duidelijk geworden dat er behoefte is aan eenvoudige en praktische hulpmiddelen. De ondernemers benadrukten het belang van standaardprocedures en vroegen om uitleg van complexe juridische termen. Ze gaven aan dat de huidige kennis en voorbereiding voor nieuwe wetgeving zoals de AI-verordening, de DGA en de CRA zelf beperkt is. In dat licht wordt de noodzaak onderstreept voor een duidelijke en toegankelijke beslisboom.

5.1.1 Vergelijking van Ontwerpeisen

De vergelijking tussen de ontwerpeisen uit het theorie-onderzoek en praktijkonderzoek laat zien dat hoewel de theoretische eisen gedetailleerd en juridisch onderbouwd zijn, de praktijkgerichtheid en toepasbaarheid centraal moeten staan in de definitieve versie van de beslisboom. Zo blijkt uit de praktijk dat ondernemers tevreden zijn met een hulpmiddel dat hen helpt het minimale te doen om aan de wettelijke vereisten te voldoen. Daarom is het essentieel om de CRA in hoofdlijnen te presenteren, zonder te vervallen in te veel details.

Binnen de praktijk zijn de verschillen tussen feedback van verschillende betrokkenen, zoals distributeurs en fabrikanten, duidelijk. Terwijl distributeurs meer gericht zijn op duidelijke uitsluitingen en conformiteit, willen fabrikanten vooral weten welke specifieke beveiligingseisen

er gelden voor hun producten. Deze variatie in feedback benadrukt de noodzaak voor een flexibel ontwerp dat aanpasbaar is aan verschillende behoeften.

Zowel uit de theorie als de praktijk komt naar voren dat het te vroeg is om uitgebreid uit te werken wanneer er bijvoorbeeld sprake is van een vermoeden van conformiteit of uitsluiting van een bepaalde product of verordening. Dit omdat de Commissie in nadere uitvoeringsbesluiten en publicaties verdere toelichting zal geven, zoals het geval bij *lex specialis* artikel 2 lid 4 CRA.[143] Dit benadrukt nogmaals een van de beperkingen van dit onderzoek, namelijk dat de CRA nog niet in werking is getreden. Dit staat in contrast met de eerste rand voorwaardelijke eisen welke een compleet en duidelijk beeld wilden geven van de CRA.[144]

5.1.2 Definitieve Ontwerpeisen

Op basis van de analyse wordt geconcludeerd dat de definitieve ontwerpeisen voor de beslisboom de volgende elementen moeten bevatten:

- Hoofdlijnen van de CRA[145]: Belangrijkste verplichtingen en procedures, zonder overmatige details. Het moet op basis van de beslisboom duidelijk zijn wat ondernemers minimaal moeten doen om hun producten op de markt te brengen.
- Standaardprocedures: Duidelijke stappen en procedures die mkb-ondernemers eenvoudig kunnen volgen. Om dit te realiseren moet bij de conclusies worden verwezen naar de standaard procedures die vanuit de Commissie zullen voortvloeien en moet bij de stappen benadrukt worden welke procedures van toepassing zijn voor de ondernemer.
- Uitleg van Termen: Gebruik van hyperlinks en korte definities om juridische termen begrijpelijk te maken. Het is van belang om bij de stappen van de beslisboom overal duidelijk te bieden.
- Flexibiliteit en Aanpasbaarheid: De mogelijkheid om de beslisboom aan te passen aan verschillende typen gebruikers, zoals fabrikanten en distributeurs. Door het opleveren van het beroepsproduct in de vorm van de software waar het in is gemaakt, kan dit naarmate amendementen worden aangepast.
- Opmaak en presentatie: Tot slot is er nog een breed aspect rondom hoe het beroepsproduct gerepresenteerd moet worden. Dit houdt o.a. in dat de tussen- en eindconclusies van de beslisboom geharmoniseerd moeten worden geformuleerd en op consistente wijze moeten worden geplaatst (op dezelfde plek onderaan). Het gebruik van hyperlinks, opsommingen, tabellen en verwijzingen dient ook op een geharmoniseerde wijze te gebeuren bij de interactieve versie, zodat de informatie helder en overzichtelijk wordt gepresenteerd. Daarnaast dienen de randvoorwaarden van de opdrachtgever als eis te worden opgenomen, zoals het opnemen van een disclaimer, het toevoegen van het logo van CSNN, en het volgen van de voorgeschreven formaten voor hoe het beroepsproduct beschikbaar is (A3-formaat, link, QR-code en softwarebestand).

143 Zie ook hoofdstuk 3.4.1.
144 Zie hoofdstuk 1.4.
145 Zoals beschreven in hoofdstuk 3.8.

Deze benadering zorgt ervoor dat de beslisboom praktisch, toegankelijk en nuttig is voor mkb-ondernemers, terwijl het voldoet aan de theoretische eisen en juridische correctheid.

5.2 Conclusie

Op basis van alle aanpassingen na de feedback van de praktijk[146], deze definitieve ontwerpeisen en de wensen van de opdrachtgever, is zowel een analoge versie als een interactieve versie van de beslisboom opgeleverd. Deze versies complementeren elkaar, de analoge versie biedt een overzichtelijke weergave welke gemakkelijk te printen en te verspreiden is. Terwijl de interactieve versie een dynamische en gebruiksvriendelijke ervaring biedt met directe toegang tot aanvullende informatie die niet kon worden opgenomen in de analoge versie. Samen zorgen zij voor een effectief hulpmiddel dat mkb-ondernemers ondersteunt bij de complexiteit van de CRA.[147]

Hoewel het onderzoek gedaan is in een vroeg stadium van de CRA en de wetgeving zich blijft ontwikkelen, is het onderzoek nu al een goede stap om vooruit te lopen op de CRA. De beslisboom biedt een overzicht van de belangrijkste vereisten en helpt ondernemers te begrijpen wanneer ze onder de CRA vallen en wat de gevolgen zijn. Er blijft echter een noodzaak voor voortdurende aanpassing en verduidelijking naarmate de EU nadere uitvoeringsbesluiten en uitleg publiceert over de CRA.

146 Zoals beschreven in hoofdstuk 4.3.
147 Zie productie 9 voor de definitieve versie.

Bronnenlijst

Baas, in: *commentaar op Richtlijn (EU) 2022/2555*
A. Baas, Lexplicatie Recht algemeen, rechtswetenschap en juridische beroepen, Deventer: Wolters Kluwer (online).

Burri & Zihlmann *Zeitschrift für Europarecht* 2023
M. Burri & Z. Zihlmann, 'The EU Cyber Resilience Act – An Appraisal and Contextualization', 2023, doi:10.36862/eiz-euz015.

Brouwer & Van Mil, *'Cybersecurity in Europa – De herziene Netwerk- en Informatierichtlijn (NIS 2)'* 2023
N. brouwer & G. van Mil, *'Cybersecurity in Europa – De herziene Netwerk- en Informatierichtlijn (NIS 2)'* **,** *NJB* 2023, afl 10, p. 748.

Brouwer & Rijneveld, *'De ontwikkeling van cyberveiligheid in Europa – Voorstel voor de Cyber Resilience Act'*, 2023.
N. Brouwer & M. Reijneveld, *'De ontwikkeling van cyberveiligheid in Europa – Voorstel voor de Cyber Resilience Act', NJB 2023,* afl 10, p. 758.

Chiara, *International Cybersecurity Law Review* 2022/3
P.G. Chiara, 'The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements', *International Cybersecurity Law Review* 2022/3, afl. 2, p. 255- 272, doi:10.1365/s43439-022-00067-6.

Cyber Risk GmbH 2024
Cyber Risk GmbH, 'The European Cyber Resilience Act (CRA)', https://www.european-cyber-resilience-act.com/, 2024.

Eckhardt & Kotovskaia, *International Cybersecurity Law Review* 2023/4
P. Eckhardt & A. Kotovskaia, 'The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive', *International Cybersecurity Law Review* 2023/4, p. 1-18, doi:10.1365/s43439-023- 00084-z.

European Commision 2023
European Commision, 'Political agreement on Cyber Resilience Act', https://ec.europa.eu/commission/presscorner, 1 december 2023.

Europees Parlement, positie van het Europees Parlement over de Cyber Resilience Act en wijzigt Verordening (EU) 2019/1020, **2022/0272(COD)** maart 2024

Europese Raad
Raad van de Europese Unie, '*Bescherming van gerubriceerde EU-informatie (EUCI)', https://www.consilium.europa.eu/nl/general-secretariat/corporate-policies/classified-information/,* 10 januari 2024.

ENISA 2019
L. Lynch e.a, *Opinion Consumers and IoT security ENISA ADVISORY GROUP*, Publication the ENISA Advisory Group's Working Group on a cybersecurity consumer perspective, 2019, https://www.enisa.europa.eu/about- enisa/structure-organization/advisory-group/ag-publications/final-opinion-enisa-ag-consumer-iot-perspective- 09.2019

ENISA 2024
H. Ramos e.a, *Cyber Resilience Act Requirements Standards Mapping*, Publication Office of the European Union, 2024, https://data.europa.eu/doi/10.2760/905934, JRC137340.

Kamerstukken II 2021/22, 21501-33, nr. 900

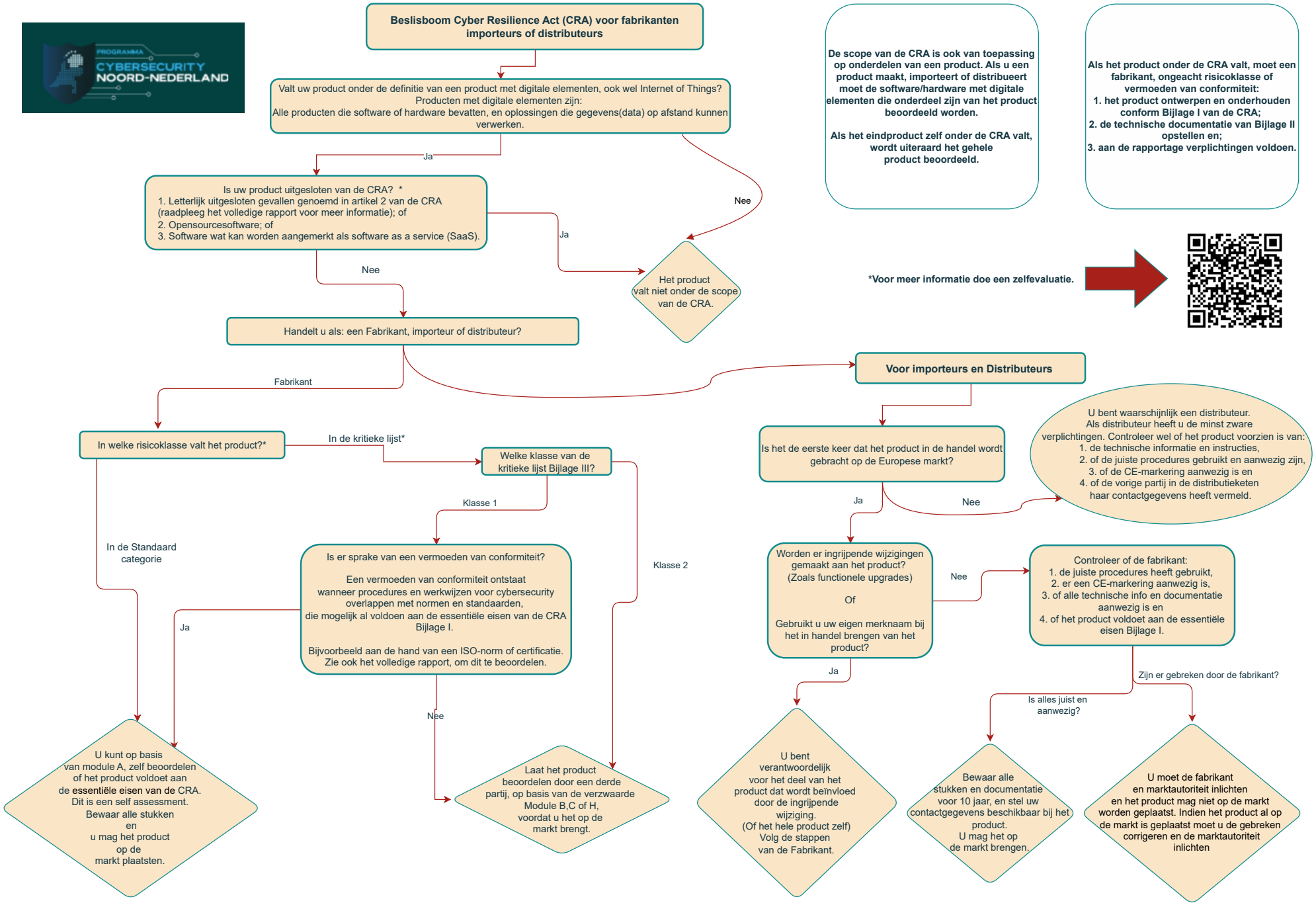
Ministerie van Economische Zaken en Klimaat
Digital trust center, '*Beveiligingstips voor Internet of Things (IoT)'*, https://www.digitaltrustcenter.nl/informatie-advies/internet-of-things-iot, datum onbekend.

Niels Norman Group
Page Laubheimer **'***Tree Testing: Fast, Iterative Evaluation of Menu Labels and Categories*', https://www.nngroup.com/articles/tree-testing/, 6 augustus 2023.

TIC Council 2022
Martin Michelot, '*TIC Council Welcomes the European Commission's Proposal for a Cyber Resilience Act', https://www.tic-council.org/news-and-events/news/press-release-tic-council-welcomes-european-commissions- proposal-cyber-resilience-act,* 16 september 2022.

Viergever & Van Til, *Computerrecht 2023*
L. Viergever & G. van Til, 'NIS2 en de AVG: werk aan de winkel?', *Computerrecht 2023*, afl. 4.

Beroepsproduct



Samenvatting en dankwoord

In een digitale samenleving waarin regelgeving zoals de Cyber Resiliance Act en de NIS2-richtlijn steeds meer impact hebben op het functioneren van organisaties, is kennisdeling geen luxe, maar een noodzaak. Ondernemers, instellingen en publieke organisaties staan voor de uitdaging om niet alleen op de hoogte te blijven van juridische verplichtingen, maar deze ook concreet en praktisch toe te passen binnen hun bedrijfsvoering. De kloof tussen juridische theorie en de dagelijkse praktijk kan groot zijn, zeker voor kleine en middelgrote ondernemingen die vaak niet over gespecialiseerde juridische of IT-afdelingen beschikken. Door complexe Europese richtlijnen en nationale wetgeving te vertalen naar toegankelijke taal en toepasbare inzichten, draagt CSNN via dit boek bij aan het versterken van digitale weerbaarheid in de regio. Bovendien wordt zichtbaar hoe regelgeving zoals de CRA en NIS2 niet alleen beperkingen opleggen, maar juist ook kansen bieden voor transparantie, vertrouwen en duurzame bedrijfsvoering voor het mkb.

Kennisdeling in dit verband betekent ook het stimuleren van samenwerking tussen onderwijs, onderzoek, bedrijfsleven en overheid. Het lectoraat speelt daarin een sleutelrol door actuele juridische kennis te verbinden aan maatschappelijke ontwikkelingen en ondernemersvragen. Door ervaringen, praktijkvoorbeelden en concrete handvatten te verzamelen en verspreiden, ontstaat een gedeelde kennisbasis die ondernemers in Groningen niet alleen ondersteunt in hun compliance, maar ook weerbaarder maakt tegen digitale dreigingen. Uiteindelijk draagt dit initiatief bij aan een cultuur van bewustwording en verantwoordelijkheid, waarin juridische regels niet langer worden gezien als obstakel, maar als essentieel onderdeel van modern ondernemerschap in een digitale economie. Kennisdeling is dan ook een investering in een veilige, transparante en toekomstbestendige bedrijfsomgeving voor iedereen.

Bij de totstandkoming van dit boek is de inzet en betrokkenheid van velen onmisbaar geweest. Allereerst willen we de studenten bedanken die met frisse blik, kritische vragen en praktische inzichten een waardevolle bijdrage hebben geleverd aan het vormgeven van de inhoud. Ook gaat onze dank uit naar de begeleiders en docenten, die met hun begeleiding, expertise en aanmoediging dit traject in goede banen hebben geleid. Een speciaal woord van dank aan de onderzoekers van het lectoraat Juridische Aspecten van het Ondernemerschap, die met hun

kennis en toewijding het fundament hebben gelegd voor de juridische duiding van de complexe materie. Tot slot danken we alle professionals, ondernemers en partners uit de praktijk die hun ervaringen en perspectieven hebben gedeeld. Dankzij deze gezamenlijke inspanning is een toegankelijk en relevant boekje ontstaan dat recht doet aan de praktijk én bijdraagt aan het versterken van juridische en digitale weerbaarheid in de regio.

mr. P. M. Piest
mr. dr. T. Mul

Titel
Cybersecurity voor het mkb: van Europese wetgeving naar regionale inbedding

Subtitel
Inzichten die de praktijk in Noord-Nederland versterken

Redactie
mr. P. M. Piest, mr. dr. T. Mulder

Auteurs
Kayleigh Veenstra, Maaike Mast, Coen Veenstra

Uitgever
CSNN

Vormgeving
The Creative Hub Groningen - powered by Canon

Druk
1e druk 150 exemplaren

share your talent.
move the world.