Onderzoek contractuele afspraken cybersecurity

1 februari 2024
Definitief rapport
Referentie: 2024/B8Z7/BvT/SS/lv/jvd

pwc

Ministerie van Economische Zaken en Klimaat

Over dit rapport

Reikwijdte

Beperkt Uitgebreid

Dit rapport heeft als doel het beantwoorden van de onderzoeksvraag van de opdrachtgever. De gestelde onderzoeksvraag luidt: 'Hoe worden cybersecurityvereisten opgenomen in B2B-contracten voor ICT-producten en diensten in Nederland?'

Wij hebben de werkzaamheden uitgevoerd zoals met u afgesproken in de opdrachtbevestiging met referentie 2023-0414/BvT/SS//jvd. In overeenstemming met de opdrachtbrief omvatte onze scope een beperkt aantal branches en een beperkt aantal ICT-leveranciers en -afnemers. We hebben een referentiekader van normenkaders en best practices uit de markt, relevante wet- en regelgeving aangaande cybersecurityovereenkomsten en het Nederlandse aansprakelijkheidsrecht, c.q. privaatrecht gehanteerd. De scope van de werkzaamheden zoals afgesproken in de opdrachtbevestiging is ongewijzigd.

Wij hebben onze analysewerkzaamheden afgerond op 9 december 2023. Dit rapport bevat daarom niet de gevolgen van gebeurtenissen na die datum, of de impact van later beschikbaar gekomen informatie.

Beschikbaarheid en kwaliteit van informatie

Geen Goed

Onze informatie is gebaseerd op een combinatie van interviews en deskresearch. Zie Appendix A voor een geanonimiseerd overzicht van de geïnterviewde organisaties en Appendix C voor een overzicht van de geanalyseerde documentatie.

De verstrekte informatie heeft ons in staat gesteld inzicht en begrip te krijgen in enkele van de belangrijkste risico's, trends en problemen rondom cybersecurity vereisten in B2B contracten en gaf een redelijke basis om de belangrijkste drijfveren en problemen te analyseren.

Conform de overeengekomen opdrachtbevestiging hebben we geen inzicht gekregen in de daadwerkelijke verschillen in de contracten. Deze contracten zijn vertrouwelijk en konden niet gedeeld worden. We hebben echter wel in de meeste gevallen de algemene voorwaarden kunnen analyseren, die openbaar beschikbaar waren op de websites van diverse organisaties.

Uitgangspunt voor ons werk

We hebben onze werkzaamheden gebaseerd op de aan ons ter beschikking gestelde informatie. Wij hebben aangenomen dat deze informatie juist, volledig en niet misleidend is. Wij hebben geen accountantscontrole uitgevoerd met betrekking tot deze informatie, noch een beoordeling gericht op het vaststellen van volledigheid en juistheid daarvan conform internationale audit- of reviewstandaarden.

Toegang tot ons rapport

Ons rapport is specifiek opgesteld voor het Ministerie van Economische Zaken en Klimaat met wie we overeenstemming hebben over het doel en de reikwijdte van ons werk of aan wie we de aard en omvang van ons werk en de beperkingen daarin hebben toegelicht. Voor het gebruik van het rapport door andere partijen dan het Ministerie van Economische Zaken en Klimaat aanvaarden wij derhalve geen verantwoordelijkheid, zorgplicht of aansprakelijkheid - contractueel, op basis van onrechtmatige daad (inclusief nalatigheid) of anderszins. Zoals overeengekomen in onze opdrachtbrief, mag ons rapport uitsluitend voor informatieve doeleinden worden gedeeld.

Overige opmerkingen

Dit rapport alsmede enig geschil voortvloeiende uit of verband houdend met (de inhoud van) het rapport worden uitsluitend beheerst door Nederlands recht.

Inhoudsopgave

1

Management samenvatting

Management samenvatting

Cybersecurityvereisten die in b2b-contracten voor ICT-producten- en diensten in Nederland worden opgenomen, hangen sterk af van de verhoudingen tussen organisaties, het kennisniveau en de risico's van de service.

Theoretisch onderzoek

Uit jurisprudentie in Nederland is gebleken dat er relatief weinig uitspraken zijn in het kader van cybersecurity en contractuele aansprakelijkheid tussen leveranciers en afnemers van ICT producten en diensten. Kanttekening hierbij is dat ons jurisprudentieonderzoek is beperkt tot de kaders van dit onderzoek, te weten een analyse van cybersecurity afspraken in b2b-contracten voor het afnemen van ICT producten en diensten, waarbij is gezocht naar geschillen tussen leveranciers en afnemers omtrent contractuele aansprakelijkheid. Over het algemeen is te zien dat het aantal rechtszaken tussen leveranciers en afnemers van ICT producten en diensten toeneemt, maar dat het nog steeds om zeer beperkte aantallen gaat, zeker in vergelijking met andere rechtsgebieden (AVG). Aan de hand van verschillende uitspraken is de zorgplicht van ICT leveranciers verder ontwikkeld (hierover meer in het Theoretisch Kader, paragraaf Zorgplicht).

Over het algemeen zien wij dat afnemers van ICT producten en diensten uit het midden- en kleinbedrijf (mkb), waar intern niet altijd voldoende kennis beschikbaar is en onvoldoende slagkracht aanwezig is ten opzichte van grote leveranciers, geen eigen inkoopvoorwaarden van toepassing kunnen verklaren voor het aanschaffen van ICT producten en diensten. Ook leveranciers uit het mkb kunnen in bepaalde verhoudingen met afnemers onvoldoende slagkracht hebben, zo kan het voorkomen dat afnemers niet de juiste budgetten ter beschikking willen stellen die nodig zijn voor het aanschaffen van de juiste dienst. Uit ons onderzoek blijkt dat onvolwassen afnemers (met bijvoorbeeld onvoldoende ICT capaciteiten en kennis) onvoldoende onderhandelingskracht hebben om goede afspraken te kunnen maken met ICT leveranciers.

Praktische bevindingen uit de interviews

De onderhandelingspositie die een organisatie (leverancier en afnemer) heeft is van essentieel belang voor het opnemen van de cybersecurity vereisten in de contracten. De vereisten die opgenomen worden in de contracten hangen sterk af van de volwassenheid van de organisatie. Onvolwassen organisaties hebben vaak geen cyberexperts die meekijken op de contracten, en zullen daardoor vaak akkoord gaan met de standaardvoorwaarden. Volwassen organisaties zullen beter in staat zijn om de eigen risico's in te schatten en hier vereisten aan te koppelen. Volwassenheid wordt doorgaans gestimuleerd door hoe kritiek de ICT infrastructuur is voor organisatie, de omvang van de organisatie, de sector en de regulering hiervan.

Een integrale risico gebaseerde benadering kan soelaas bieden, ook voor kleinere organisaties. In de contracteringsfase zijn er verschillende redenen om voorwaarden wel of niet op te nemen. De belangrijkste reden is het risico dat gepaard gaat met een bepaalde ICT dienst en de impact op kritieke infrastructuur van organisaties. Bij minimale risico's zullen over het algemeen ook de vereisten minder hoog zijn. Een andere reden die vaak een rol speelt in business-to-business (hierna: b2b) contracten zijn de kosten die gemoeid gaan met de service die geboden wordt. Extra voorwaarden, vereiste certificeringen en/of Service Level Agreements (hierna: SLAs) behoren vaak wel tot de mogelijkheden maar betekenen dat de kosten van het contract omhoog gaan.
Andere redenen voor leveranciers om standaard hoge securitymaatregelen in te regelen zijn de eventuele reputatieschade in het geval van een incident en het ontzorgen van de kritieke (zoals gedefinieerd in de Network and Information Security directive 2 (NIS2)) mkb bedrijven. Bedrijven zoeken hierbij naar een evenwicht tussen de voordelen van security op basis van de risico's.

Wanneer we kijken naar Maatschappelijk Verantwoord Ondernemen en aankomende regelgeving (bijv. NIS2) zien we een algemene ontwikkeling dat leveranciers een bepaald concurrentievoordeel kunnen behalen door zich te positioneren als een bedrijf dat op verantwoorde wijze omgaat met de data. Zo worden zij al snel beschouwd als betrouwbare samenwerkingspartner.

Knelpunten die het lastig maken om de cybersecurity maatregelen te bepalen zijn ten eerste het gebrek aan onderhandelingskracht van een organisatie. Ten tweede, zorgt beperkt bewustzijn binnen organisaties over de ICT risico's voor het sneller akkoord gegaan met standaardeisen, of onredelijk zware eisen. Dit draagt eraan bij dat in veel gevallen de verantwoordelijkheden in het omgaan met incidenten niet duidelijk gedefinieerd worden. Ten derde is het vaak onduidelijk tot hoever de zorg(plicht) van de leverancier en afnemer gaat. Veel leveranciers zijn bereid te helpen en mee te denken maar voelen zich niet verantwoordelijk voor hoe een afnemer hun omgeving/applicatie gebruikt. Dit wordt ook bij de meest recente geschillen zo beoordeeld, waarin gesteld wordt dat er ook een verantwoordelijkheid bij de afnemer van een dienst ligt. Tot slot is de huidige samenwerking met een organisatie vaak beslissend voor de contracten. Wanneer contracten al lang lopen en de afnemer afhankelijk is van de service van de leverancier, zal er weinig ruimte zijn voor additionele vereisten in de contracten.

Mogelijke beleidsinstrumenten

De organisaties hebben verschillende beleidsinstrumenten genoemd die wenselijk zijn. Ten eerste moet ervoor gezorgd worden dat er een centrale plek is waar duidelijke en concrete voorbeelden worden gegeven van best practices in de markt om cybersecurity te verbeteren. Ten tweede moet er aangestuurd worden op het belang van standaardisering en harmonisatie. Hierbij worden duidelijke kaders verwacht voor wet- en regelgeving rondom contractuele afspraken, waarbij zo veel mogelijk harmonisatie bestaat tussen verschillende binnen- en buitenlandse regels. Tot slot zou een sociaal vangnet gecreëerd moeten worden waar organisaties terecht kunnen wanneer zij ernstige digitale schade lijden.

2

Introductie

Inleiding onderzoek (1/2)

Een omschrijving van de vraag en onze bijdrage

Startpunt van het onderzoek

Het Ministerie van Economische Zaken en Klimaat (hierna: EZK) werkt aan een duurzaam en ondernemend Nederland, en geeft ondernemers de ruimte om te vernieuwen en de economische kansen van verduurzaming en digitalisering te benutten.

Vanuit de Nederlandse Cybersecuritystrategie (hierna: NLCS) en het rapport van de Onderzoeksraad voor Veiligheid (hierna: OVV) is de behoefte ontstaan om een onderzoek te starten naar de verkenning van hoe het maken van heldere contractuele afspraken tussen leverancier en afnemers (b2b) van Informatie- en Communicatietechnologie (hierna: ICT)-diensten en -producten kan worden gestimuleerd (en gestandaardiseerd). Dit onderzoek ondersteunt de beleidsdoelstellingen uit de NLCS om de digitale weerbaarheid van organisaties te vergroten en ICT-producten en -diensten veiliger te maken (Apache Log4J was een goed voorbeeld van de impact die een software kwetsbaarheid kan hebben op duizenden organisaties). Een mix aan beleidsinstrumenten is hiervoor nodig op nationaal en Europees niveau.

In het rapport heeft de OVV aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de minister van EZK (ten behoeve van alle organisaties en consumenten in Nederland) de volgende aanbeveling gedaan: bevorder dat Nederlandse organisaties en consumenten gezamenlijk veiligheidseisen formuleren en afdwingen bij softwarefabrikanten.

Hiernaast is vanuit het werkveld de behoefte geuit aan een betere inzet op de bewustwording van bedrijven. Afnemers zouden graag meer duidelijkheid hebben over wat goede cybersecurity clausules zijn, om op te nemen in contracten voor ICT-producten en -diensten. Leveranciers worden graag voorzien van kennis en instrumenten waarmee goede contracten afgesloten kunnen worden.

Dit onderzoek heeft zich gericht op twee groepen: het midden- en kleinbedrijf en de grotere bedrijven in Nederland. De onderzoeksvraag voor dit project is daarom: *“Hoe worden cybersecurityvereisten opgenomen in b2b-contracten voor ICT-producten- en diensten in Nederland?“.*

De beantwoording van de hoofdvraag zal geschieden aan de hand van vijf deelonderwerpen. In de volgende sectie worden deze deelonderwerpen toegelicht.

De doelstelling van deze opdracht (‘output’) is om een onderzoek uit te voeren naar de cybersecurityvereisten opgenomen in b2b-contracten voor ICT-producten en -diensten in Nederland, in verschillende branches en bij zowel grote bedrijven als het mkb. Dit wordt gerealiseerd aan de hand van het beantwoorden van de hoofdvraag, kijkend naar vijf deelonderwerpen. Hieruit worden inzichten verkregen over hoe een relevante set aan cybersecurityvereisten eruitziet voor individuele organisaties en specifieke sectoren. Dit onderzoek draagt bij (‘outcome’) aan de beleidsdoelstellingen uit de NLCS. Het referentiekader voor de uitvoering van de opdracht betreffen normenkaders en best practices uit de markt, relevante wet- en regelgeving aangaande cybersecurityovereenkomsten en het Nederlandse aansprakelijkheidsrecht, c.q. privaatrecht.

Aanpak van het onderzoek

Het onderzoek is uitgevoerd tussen 11 september 2023 en 22 december 2023, waarbij de volgende fasering is aangehouden.

Fase 1 - De documentatie- en literatuurstudie had als doel om op hoofdlijnen de kaders van het verdere onderzoek aan te scherpen, in het bijzonder de bedrijven/organisaties die wij voornemens waren te benaderen.

Fase 2 – De interviews en contractanalyse hadden het doel om de informatie over de contractuele vereisten en de totstandkoming van deze vereisten op te halen die wij op basis van de documentatiestudie niet hebben kunnen verkrijgen.

Fase 3 – Analyse en Validatie zijn gedaan om de resultaten uit de documentatiestudie, interviews en contractanalyse verder te analyseren. Er is gekeken naar de status quo van de vereisten in contracten, de overeenkomsten en verschillen tussen contracten van bedrijven en sectoren, de knelpunten waar levernaciers en afnemers tegenaan lopen, en mogelijke instrumenten en relevante prikkels voor de stimulering van contractuele afspraken.

Fase 4 – Rapportage en eindpresentatie geven een algemeen beeld van de bevindingen van het onderzoek waarbij de hoofdvraag wordt beantwoord.

Inleiding onderzoek (2/2)

Een omschrijving van de vraag en onze bijdrage

Overige punten

Dit document is opgesteld in opdracht van EZK. Dit document wordt u aangeboden vanuit PricewaterhouseCoopers Advisory N.V. Het betreft dus geen document opgesteld door accountants. Wij hebben aangereikte informatie (zowel schriftelijk als mondeling) dan ook voor juist en volledig aangenomen en hier geen controle of andere vorm van toetsing op uitgevoerd. Met deze rapportage verstrekken wij geen accountantsverklaring, -certificering of andere vorm van zekerheid, met betrekking tot de door ons verleende diensten of de informatie op basis waarvan onze diensten zijn verleend. Wij hebben de informatie die aan ons door welke bron dan ook in het kader van de opdracht is verstrekt, niet onderworpen aan een accountantscontrole of op andere wijze geverifieerd.

Onze werkzaamheden vormen geen onderzoek zoals bedoeld in de algemeen aanvaarde richtlijnen met betrekking tot controleopdrachten. In het kader van deze opdracht worden wij niet geacht op de hoogte te zijn van informatie die aan andere vertegenwoordigers van PwC dan die betrokken bij de uitvoering van deze opdracht is verstrekt.

U blijft te allen tijde zelf volledig verantwoordelijk voor eventuele op dit document gebaseerde besluitvorming en/of beslissing(en). PwC aanvaardt geen enkele aansprakelijkheid (ook niet voor nalatigheid) voor de gevolgen van enig handelen of nalaten door u en/of derden op basis van (de inhoud van) dit document, en wijst iedere verantwoordelijkheid, zorgplicht en/of aansprakelijkheid – contractueel, op basis van onrechtmatige daad (inclusief nalatigheid) of anderszins – af voor enig besluit en/of enige beslissing waaraan (de inhoud van) dit document ten grondslag ligt.

Deze publicatie alsmede enig geschil voortvloeiende uit of verband houdend met (de inhoud van) deze publicatie worden uitsluitend beheerst door Nederlands recht.

Deze opdracht is uitgevoerd onder de overeenkomst van 7 september 2023, met ons kenmerk 2023-0414/BvT/SS//jvd.

Leeswijzer

Deze rapportage is opgebouwd uit verschillende hoofdstukken. In Hoofdstuk 3 wordt de methode nader toegelicht die wij gehanteerd hebben. In Hoofdstuk 4 worden de deelvragen beantwoord. In elk deelonderwerp komen (dezelfde) gerichte sub-onderwerpen terug, (bijv. verhoudingen tussen afnemer en leverancier en kennisniveau) die meerdere deelonderwerpen raken, die tot slot leiden tot de belangrijkste adviezen uit Hoofdstuk 5. In de bijlage staan we stil bij bijvoorbeeld de rationale voor het betrekken van bepaalde sectoren, en de planning van dit onderzoek.

3

Methode

Achtergrond en toelichting

De doelstelling van het project is het uitvoeren van een marktonderzoek naar de volgende vraag:

“Hoe worden cybersecurityvereisten opgenomen in b2b-contracten voor ICT-producten- en diensten in Nederland?”

Deze vraag wordt beantwoord aan de hand van **5 deelonderwerpen:**

1. Een omschrijving van de praktijk van cybersecurityvereisten in contracten van ICT-producten en -diensten tussen leveranciers en afnemers uit het mkb en grotere bedrijven in Nederland.
2. Indien niet aanwezig, een omschrijving van redenen waarom contractuele vereisten niet zijn opgenomen.
3. Indien aanwezig, omschrijving van de invulling van deze vereisten.
4. Omschrijving van knelpunten waar leveranciers en afnemers tegenaan lopen op gebied van cybersecurity.
5. Overzicht van mogelijke (beleids-)instrumenten en relevante prikkels voor het stimuleren van heldere contractuele afspraken op gebied van cybersecurity.

Bronnen

Om de verschillende deelonderwerpen goed inzichtelijk te krijgen zijn verschillende bronnen gebruikt. Interviews met leveranciers en afnemers van ICT-diensten of –producten zijn afgenomen, een onafhankelijke onderzoeksorganisatie is gevraagd naar hun inzichten, en relevante documentatie is bestudeerd.

Bestudeerde documentatie

- Bestaande rapporten over contractuele cybersecurity afspraken
- (Inter)nationale wet- en regelgeving
- Jurisprudentie
- Kronieken

*Verdere toelichting van de geanalyseerde documentatie is te vinden in Appendix C.

Interviews

Wij hebben verschillende organisaties geïnterviewd over hun kijk op cybersecurity vereisten in contracten. Hierbij hebben wij gekozen voor een diverse groep aan afnemers en leveranciers. De diversiteit komt voort uit de verschillende sectoren waar deze uit komen en de omvang van de organisaties. Een duidelijkere omschrijving van de onderzoeksgroep wordt gegeven op de volgende pagina.

Aanvullend gevoerde gesprekken

Aanvullend op de organisaties die wij geïnterviewd hebben, hebben wij ook gesproken met:

- Onderwerp specialisten binnen een onderzoeksorganisatie of onderzoekers: TNO.
- Een klankbordgroep, met afgevaardigden van:
  - CIO Platform Nederland
  - NLdigital
  - Stichting DINL
  - VNO-NCW

Interviews: Onderbouwing van de onderzoeksmatrix

Een onderbouwing voor de keuze voor sectoren en de gekozen verhoudingen tussen afnemers/leveranciers en organisatieomvang

Bij het kiezen van organisaties is er gekeken naar variatie in sector en omvang van de organisatie. In onderstaande tabel zijn de aantallen per afnemer, leverancier, en sector te zien.

- Definities van sectoren en omvang zijn gebaseerd op Europese standaarden (22 sectoren totaal).[1]
- Geen microbedrijven: gezien de verwachting van relatief weinig eigen sturing op inhoud van contracten (inzake cybersecurity) waarbij vaak aansluiting wordt gezocht bij standaard templates.
- Geen ondernemingen die gelijk kunnen worden gesteld met consumenten en daardoor onder de consumentenbescherming vallen.
- Weinig reeds (sterk) gereguleerde sectoren t.a.v. cybersecurity, zoals Rijksoverheid en organisaties aangewezen als kritische infrastructuur.
- Diversiteit in sectoren.

Sectoren afnemers: Één afnemer per sector: Productie, transport, uitgever, financieel, technische ondersteuning, publieke administratie, zorg en cultuur.	**Omvang afnemers:** • Vier grote afnemers van ICT-producten en -diensten; • Vier mkb afnemers van ICT-producten en –diensten.
Sectoren leveranciers: • Twee leveranciers van softwareproducten; • Drie leveranciers van clouddiensten; • Twee leveranciers van ICT-infrastructuurdiensten.	**Omvang leveranciers:** • Drie grote leveranciers van ICT-producten en -diensten; • Vier mkb leveranciers van ICT-producten en –diensten.

* De verdere onderbouwing van classificatie en de onderzoeksmatrix voor de omvang en de sectoren is te vinden in Appendix A.

4

Resultaten & observaties

Theoretisch kader (1/3)

Een omschrijving van de documentatie- en literatuurstudie

Startpunt van het onderzoek

Om de kaders voor het onderzoek aan te scherpen en als voorbereiding op de interviewfase, is er een documentatie- en literatuurstudie uitgevoerd (zie appendix C). Onderdeel hiervan was het bestuderen van reeds bestaande onderzoeken op dit vlak om bestaande inzichten en theorieën te identificeren. Ook is wet- en regelgeving op hoofdlijnen bestudeerd en is onderzoek gedaan naar jurisprudentie op het gebied van cybersecurity en aansprakelijkheid in dit verband. Daarnaast is er een contractenanalyse uitgevoerd ten aanzien van cybersecurity en aansprakelijkheid in algemene voorwaarden van ICT leveranciers en afnemers die (online) door de geïnterviewde organisaties ter beschikking zijn gesteld. Hierbij verdient het op te merken dat wij, onder meer vanwege vertrouwelijkheid, niet de daadwerkelijke contracten (waar de algemene voorwaarden op van toepassing zijn), hebben bekeken. In beginsel is vaak het uitgangspunt dat de bepalingen in een contract voorrang hebben boven de bepalingen in de algemene voorwaarden. Daarom valt niet uit te sluiten dat leveranciers en afnemers in de contracten van bepaalde delen van de algemene voorwaarden zijn afgeweken. Uit de interviews en literatuur is gebleken dat dergelijke maatwerkcontracten (met afwijkende voorwaarden) vaak worden onderhandeld bij projecten met grote (commerciële) omvang en tussen grote/deskundige partijen. Bij kleinere projecten en bij kleinere afnemers worden regelmatig enkel algemene voorwaarden van toepassing verklaard samen gaand met een inkooporder. Dit alles is uiteindelijk mede inkleurend bij het bepalen van de reikwijdte van de zorgplicht van leveranciers, waar op de volgende pagina op wordt uitgeweid.

Het theoretisch kader dient als startpunt voor het verdere onderzoek, waarbij onze bevindingen zijn getoetst tijdens de interviews in de volgende fase.

Bestaande rapporten

Cybersecurity is een actueel en dynamisch onderwerp, gezien de toenemende frequentie en diversiteit van cyberaanvallen en de groeiende afhankelijkheid van bedrijven (maar ook personen) van ICT producten en diensten. Cybersecurity is ook een thema waar veel factoren samenkomen, zoals technische capaciteiten en veiligheid van ICT producten en diensten, juridische kaders van geldende wet- en regelgeving op het gebied van cybersecurity en het handelen van bedrijven / personen en eventuele schade en aansprakelijkheden die daaruit voortvloeien.

Dit volgt onder meer uit de reeds bestaande rapporten en onderzoeken waar wij kennis van hebben genomen, zoals het rapport “Nederlandse cybersecuritystrategie 2022 - 2028”, het rapport "*Good practices for supply chain cybersecurity*" en het onderzoek “*Aansprakelijkheid voor digitale onveiligheid in b2b-relaties*”. In laatstgenoemde onderzoek is onderzocht of het Nederlandse aansprakelijkheidsrecht voldoende mogelijkheden biedt om in een b2b-relatie cybersecurity schade te verhalen. De conclusie was onder andere dat de juridische en economische barrières vaak te groot zijn om verhaal praktisch mogelijk te maken en dat beoordeeld moet worden of overheidsbeleid de juridische en economische barrières (deels) kan wegnemen.

Wet- en regelgeving en jurisprudentie

Cybersecurity wordt beïnvloed door zowel nationale als internationale wet- en regelgeving die wij voor ons onderzoek op hoofdlijnen hebben bestudeerd. Denk daarbij aan de Cyber Resilience Act, Cybersecurity Act en de Radio Equipment Directive voor wat betreft de Europese regelgeving die er deels al is en er deels aankomt. Denk daarnaast aan het Burgerlijk Wetboek op nationaal niveau en de Algemene Verordening Gegevensbescherming met directe werking.

Ons jurisprudentieonderzoek is beperkt tot de kaders van ons onderzoek, te weten een analyse van cybersecurityvereisten in b2b-contracten voor het afnemen van ICT producten en diensten, waarbij wij nadrukkelijk hebben gezocht naar geschillen tussen leveranciers en afnemers omtrent aansprakelijkheid. Uit ons jurisprudentieonderzoek is gebleken dat er relatief weinig uitspraken zijn in het kader van cybersecurity en aansprakelijkheid tussen leveranciers en afnemers van ICT producten en diensten. Over het algemeen is wel te zien dat rechtszaken tussen leveranciers en afnemers van ICT producten en diensten toenemen maar dat het nog steeds om zeer beperkte aantallen gaat, zeker in vergelijking met andere rechtsgebieden (AVG) en dat dit vaak bredere ICT-vraagstukken betreft. De rechtbank Overijssel heeft op 10 mei 2023 een uitspraak gedaan die aanknopingspunten gaf voor ons onderzoek. In de zaak gemeente Hof van Twente, oordeelde de rechtbank dat er, bij eventuele schade als gevolg van een cyberaanval, ook een zekere mate van verantwoordelijkheid ligt bij de afnemer bij het gebruik van ICT producten en diensten en dat de verantwoordelijkheden en zorgplicht van de ICT leverancier (bijvoorbeeld ten aanzien van monitoring op beveiligingsrisico's) mede afhankelijk is van de contractuele afspraken tussen partijen. De partijen hadden in deze zaak geen contractuele afspraken gemaakt over het melden van beveiligingsrisico's door de leverancier, maar wel om risicovolle situaties te detecteren. Volgens de rechter had Hof van Twente als afnemer een (groot) aandeel in ransomware-aanval door onder meer de rdp-poort (een onderdeel dat het mogelijk maakt om op afstand te verbinden met een computer of server) naar het internet open te zetten, een eenvoudig te raden wachtwoord in te stellen en geen tweestapsverificatie te hanteren.

Theoretisch kader (2/3)

Een omschrijving van de documentatie- en literatuurstudie

Contractenanalyse

Ter voorbereiding op de interviews hebben wij, voor zover deze online beschikbaar waren, algemene voorwaarden van leveranciers en afnemers bestudeerd voor wat betreft afspraken over cybersecurity en aansprakelijkheid. Zoals hiervoor reeds vermeld, hebben wij niet de daadwerkelijke contracten (waar de algemene voorwaarden op van toepassing zijn) bekeken.

In de leverings/verkoopvoorwaarden van leveranciers zien wij over aansprakelijkheden op het gebied van cybersecurity dat leveranciers in het algemeen de aansprakelijkheid voor schade als gevolg van schending van cybersecurity volledig uitsluiten (tenzij er sprake is van opzet of grove schuld) of zoveel mogelijk beperken. Dit wordt ook bevestigd in het eerder besproken onderzoek “Aansprakelijkheid voor digitale onveiligheid in b2b-relaties”. Vaak wordt in de leveringsvoorwaarden van leveranciers ook niet gegarandeerd dat de diensten altijd ononderbroken en foutloos zullen functioneren. Ter nuancering verdient het op te merken dat het hier gaat om leveringsvoorwaarden die ICT leveranciers zelf hebben opgesteld/ hebben laten opstellen door externe juristen (dus anders dan de hierna te bespreken NLdigital voorwaarden).

In de inkoopvoorwaarden van afnemers zien wij dat geprobeerd wordt een zekere mate van garantie af te dwingen over de werking van de af te nemen ICT producten en diensten. Welke set algemene voorwaarden uiteindelijk van toepassing is op de contractuele verhoudingen is afhankelijk van een aantal factoren, zo is gebleken uit de interviews (zoals de slagkracht en omvang van de contracterende organisaties).

In de interviewfase is als een van de thema's aan bod gekomen in welke mate over algemene voorwaarden tussen partijen wordt onderhandeld en in hoeverre hierover geschillen ontstaan. Zoals hierna bij de uitwerking van de interviews ook zal blijken (en zoals ook uit ons jurisprudentieonderzoek is gebleken en eveneens opgemerkt in het onderzoek “Aansprakelijkheid voor digitale onveiligheid in b2b-relaties”) worden geschillen zelden beslecht voor de rechter. Organisaties proberen er zoveel mogelijk samen uit te komen, waardoor een gang naar de rechter vaak uit blijft.

NLdigital voorwaarden

Naast de online beschikbare algemene voorwaarden van leveranciers en afnemers, hebben wij tevens de NLdigital voorwaarden bestudeerd, die worden gebruikt door meerdere bedrijven die actief zijn in (of gebruik maken van) de ICT sector. De NLdigital voorwaarden zijn opgesteld vanuit het perspectief van de leverancier. Zo is op de website te lezen: "*Als bedrijf in de digitale sector zorg je voor uitstekende dienstverlening aan jouw klanten. Mocht er onverhoopt toch iets misgaan, dan kunnen jouw opdrachtgevers je aansprakelijk stellen. Met de NLdigital voorwaarden hoef je je geen zorgen te maken over aansprakelijkheidskwesties omdat je goed beschermd bent.*"

Zonder naar volledigheid te streven, is er in de NLdigital voorwaarden te zien dat de aansprakelijkheid van leveranciers is beperkt tot een bepaald bedrag (voor wat betreft directe schade) of uitgesloten (voor wat betreft indirecte schade), tenzij er sprake is van opzet of bewuste roekeloosheid. Verder staat er in de NLdigital voorwaarden dat de leverancier er niet voor in staat dat een Software as a Service-dienst (hierna ‘SaaS-dienst’) foutloos is, zonder onderbrekingen functioneert en tijdig wordt aangepast aan wijzigingen in relevante wet- en regelgeving. Kanttekening hierbij is dat het uitgangspunt van de NLdigital voorwaarden een inspanningsverplichting is en niet een resultaatverplichting.

Wel is te verwachten dat, zoals hiervoor kort beschreven, de NLdigital voorwaarden mogelijk gebruikt worden door (kleine) ICT leveranciers die vaak afhankelijk zijn van hun afnemers. Zo is op de website van NLdigital is te lezen: "*De NLdigital voorwaarden zijn dé standaard algemene voorwaarden voor de ICT-branche. Ze worden ingezet door 2.000 IT-bedrijven in Nederland en dekken alle essentiële thema’s.*" Hoewel ook daarvoor geldt dat de NLdigital voorwaarden in beginsel meer in het voordeel zijn van de ICT leverancier, is de mate van voordeel sterk afhankelijk van de partij waarmee gecontracteerd wordt en de voorwaarden die uiteindelijk uit-onderhandeld worden door de partijen in het contract waar de NLdigital voorwaarden op van toepassing worden verklaard.

Theoretisch kader (3/3)

Een omschrijving van de documentatie- en literatuurstudie

Zorgplicht

Over het algemeen wordt de levering van ICT diensten gedaan op basis van een overeenkomst van opdracht, waarbij de leverancier de opdrachtnemer is en de afnemer de opdrachtgever is. De overeenkomst van opdracht is in de wet geregeld (art. 7:400 e.v. Burgerlijk Wetboek), waarbij in de wet is vastgelegd dat de opdrachtnemer (zijnde de leverancier) bij de uitvoering van de opdracht de zorg van een goed opdrachtnemer in acht moet nemen (art. 7:401 Burgerlijk Wetboek). Op grond van de wet rust er dus een zorgplicht op de opdrachtnemer. Hoe en wanneer er precies gesproken kan worden van een 'goed opdrachtnemer' is mede afhankelijk van de afspraken met de opdrachtgever (zijnde de afnemer). Uit jurisprudentie volgt dat daarbij de maatstaf is hoe een redelijk bekwaam en redelijk handelend ICT leverancier in die situatie te werk zou zijn gegaan (ECLI:NL:GHAMS:2020:1987). Een praktijkvoorbeeld hiervan is een zaak waarbij de rechtbank oordeelde dat van een bekwaam en redelijk handelend ICT leverancier verwacht mag worden dat zij een afnemer waarschuwt als de door de afnemer gewenste wijzigingen in de ICT dienst de functionaliteiten zodanig zou aantasten dat deze niet meer zou functioneren (ECLI:NL:RBROT:2022:1641).

De zorgplicht van leveranciers van ICT producten en diensten is mede afhankelijk van de aard, omvang en complexiteit van de ICT producten en diensten die leveranciers aanbieden en de contractuele afspraken die hierover zijn gemaakt. Hierdoor kan de zorgplicht van een leverancier uitgebreid of juist beperkt zijn. Daarbij is het van belang dat de ICT producten en diensten die worden geleverd voldoen aan de overeengekomen specificaties, functionaliteiten en kwaliteitseisen en dat alle overeengekomen afspraken worden nagekomen.

De leverancier heeft in het algemeen de zorgplicht om te voldoen aan de in de overeenkomst vastgelegde eisen. Als een leverancier niet voldoet aan de in de overeenkomst overeengekomen afspraken, dan is er sprake van een tekortkoming in de nakoming van diens verplichtingen uit de overeenkomst. Wanneer de tekortkoming in de nakoming toe te rekenen is aan de leverancier is er sprake van wanprestatie (c.q. het schenden van een verplichting in een overeenkomst), op grond waarvan de afnemer schade zou kunnen verhalen op de leverancier.

De drempel voor verhaalsmogelijkheden kan echter groot zijn, omdat leveranciers, zoals hiervoor reeds besproken, in contracten vaak geen resultaatsverplichting aangaan en geen garantie geven over de werking van de af te nemen ICT producten en diensten. Ter nuancering: de werking van ICT producten en diensten is mede afhankelijk van de aard van het te kopen product en de af te nemen dienst, de overeengekomen specificaties en functionaliteiten en de op basis daarvan gewekte verwachtingen bij afnemers. Omdat er geen resultaatsverplichting overeengekomen wordt, maar een inspanningsverplichting, is het niet eenvoudig om vast te stellen dat een leverancier zich onvoldoende heeft ingespannen om een contractuele afspraak na te komen.

Aanvullend op de hiervoor beschreven wettelijke zorgplicht uit art. 7:401 Burgerlijk Wetboek is in de rechtspraak de bijzondere zorgplicht ontstaan. Dit is een verzwaarde zorgplicht voor een ICT leverancier die wordt geacht meer deskundig te zijn dan een afnemer. Afhankelijk van de overeengekomen afspraken en de omstandigheden van het geval, kan er sprake zijn van een invulling van de zorgplicht aan de hand van verschillende situaties, zoals bijvoorbeeld het voldoen aan de informatie- en waarschuwingsplicht, de overeengekomen functionaliteiten en specificaties, het begeleiden bij ontwikkelingen / updates, de nazorgplicht en het zorgdragen voor back-up van data. De omvang van de verzwaarde zorgplicht van de ICT leverancier kan echter ook genuanceerd worden naarmate de afnemer ook een zekere mate van deskundigheid bezit (ECLI:NL:GHAMS:2020:2016).

Zoals reeds eerder opgemerkt, is over het algemeen te zien dat rechtszaken tussen leveranciers en afnemers van ICT producten en diensten toenemen. Mede aan de hand van verschillende uitspraken is de (bijzondere) zorgplicht van ICT leveranciers verder ontwikkeld in de rechtspraak. Volledigheidshalve wordt opgemerkt dat bij het bespreken van de (inkleuring van de zorgplicht langs de lijn van de) jurisprudentie er niet gestreefd is naar volledigheid, maar alleen die zaken zijn bestudeerd die meer duidelijkheid geven over de zorgplicht en die voor onze onderzoeksvraag relevant zijn (te weten geschillen omtrent aansprakelijkheid als gevolg van het niet nakomen van cybersecurityvereisten in b2b-contracten bij het afnemen van ICT producten en diensten).

Deelonderwerp 1 – cybersecurityvereisten in contracten (1)

Een omschrijving van de praktijk van cybersecurityvereisten in contracten van ICT-producten en diensten tussen leverancier en afnemers uit het mkb en grotere bedrijven in Nederland

B2b contractonderhandelingen over cybersecurity verschillen tussen contracterende organisaties. Verschillen worden voornamelijk veroorzaakt door de verhouding tussen organisaties, de commerciële waarde van het contract, de dienstverlening, de verwachtingen van afnemers, het kennisniveau, en de regulering.

De verhoudingen tussen de contracterende organisaties zijn vaak bepalend bij de contractonderhandelingen voor het afnemen van ICT-producten en diensten. Wanneer een van de twee partijen hierin een (zwaar) overwicht heeft werkt dit door op de slagkracht die de organisatie heeft bij het opnemen van cybersecurityvereisten en bijbehorende aansprakelijkheden in contracten, zoals algemene voorwaarden, Master Service Agreements (hierna: MSAs) of SLA. Het overwicht wordt bepaald door commerciële waarde van de opdracht, maar ook door het kennisniveau van de partijen en de afhankelijkheid van het type dienstverlening. Zo zien wij dat mkb afnemers over het algemeen geen eigen inkoopvoorwaarden van toepassing kunnen verklaren voor het aanschaffen van ICT producten en diensten, maar ook leveranciers uit het mkb kunnen onvoldoende slagkracht hebben, zo kunnen afnemers bezwaar hebben als er extra geld uitgegeven moet worden aan noodzakelijke beveiliging. Aan de andere kant zijn er ook kleine afnemers met een groot marktaandeel (niche product) en een hoog kennisniveau. Deze afnemers zijn hierdoor minder afhankelijk van een leverancier waardoor voorwaarden gelijkwaardiger onderhandeld kunnen worden. Daarnaast kan de slagkracht van een afnemer een boost krijgen door samenwerking met brancheorganisaties.

Afhankelijk van het type dienstverlening en het daarmee gepaarde risico wordt vaak uit voorzorg (zorgplicht) door de leverancier bepaalde functionaliteit technisch dichtgezet. Dit om te voorkomen dat er bijvoorbeeld door de afnemer een koppeling wordt gemaakt met applicaties die niet door de leverancier op een white list zijn gezet, en daarmee als “veilig” worden bestempeld.

De verwachtingen van afnemers van ICT diensten varieert sterk per dienst die afgenomen wordt. Afhankelijk van het doel en het risicoprofiel van de diensten en producten die afnemer nodig heeft (welke informatie wordt er verwerkt/gaat het om systemen voor de kerntaken van de afnemer) zouden afnemers specifieke eisen aan de cybersecurity voorwaarden c.q. maatregelen van de leverancier moeten stellen. Niet elke afnemer is echter in staat of heeft de mogelijkheid om de risico's goed in te schatten, om daar vervolgens passende contractuele voorwaarden aan te verbinden met leveranciers.

Het kennisniveau van de contracterende organisatie is van groot belang, om in staat te zijn de cyber risico’s en de benodigde maatregelen te identificeren. Veel organisaties (voornamelijk mkb) hebben beperkte (financiële) middelen om in te zetten voor het inbouwen van cybersecurity maatregelen (denk hierbij ook aan het tekort aan technisch personeel). Daarnaast is vaak niet de kennis aanwezig om contractuele onderhandelingen goed te kunnen voeren op de onderwerpen die risico’s verkleinen. Wanneer dit kennisniveau er wel is worden er meer inhoudelijkere discussies gevoerd die beide partijen verder helpen. In sommige gevallen leidt dit zelfs tot partnerships, waarbij afnemer en leverancier elkaar ondersteunen en informatie delen om samen een hoger kennisniveau te bereiken. Bij een partnership wordt in het algemeen door de leverancier meer overlegd gevoerd met de afnemer en worden concrete plannen gemaakt. Intensieve samenwerking zien we naast grote partnerships ook veel voorkomen bij kleine leveranciers.

Deze kleinere leveranciers staan in een partnership vaak in nauw contact met de afnemers, waarbij maatwerk en tussentijdse evaluatie dan staan centraal. Doordat kleinere leveranciers vaak minder certificeringen hebben, en minder gemonitord en geaudit worden lijkt de volwassenheid van kleine leveranciers voor afnemers lager te zijn. Dit leidt tot de keuze tussen meer maatwerk met minder schijnbare cyberveiligheid, of minder maatwerk en een meer volwassen omgeving. In de praktijk zien wij dat ook kleine leveranciers volwassen kunnen zijn. Wel lijkt het gebrek aan volwassen cyberkennis in bepaalde (niet gereguleerde) sectoren groter te zijn dan bij andere sectoren.

Regulering van bepaalde organisaties/sectoren zorgt voor een stimulans in het bewustzijn van de organisatie (denk aan de financiële sector, verzekeringsbranche of essentiële sectoren). Deze regulering kan komen vanuit de overheid, maar ook uit overkoepelende organisaties en/of samenwerkingsverbanden. Wanneer een organisatie gereguleerd wordt, is een duidelijk kennisverschil op te merken (compliance-driven). Bij deze organisaties worden doorgaans ook beter de risico’s in kaart gebracht. Dit is ook te merken in de verwachtingen die zij hebben van leveranciers en de daarbij behorende contractuele afspraken die gemaakt worden. Hierbij is op te merken dat afnemers bij het selecteren van nieuwe leveranciers meer waarde hechten aan de maatregelen die worden genomen door de leverancier dan aan de contractuele afspraken die daaromheen gelden. Daarnaast heeft veel nieuwe wetgeving (waaronder de NIS2 directive) vereisten over het beoordelen van de keten van leveranciers. Hierdoor krijgen steeds meer organisaties te maken met vereisten uit deze regulering.

Deelonderwerp 1 – cybersecurityvereisten in contracten (2)

Een omschrijving van de praktijk van cybersecurityvereisten in contracten van ICT-producten en diensten tussen leverancier en afnemers uit het mkb en grotere bedrijven in Nederland

B2b contractonderhandelingen over cybersecurity verschillen tussen contracterende organisaties. Verschillen worden voornamelijk veroorzaakt door de verhouding tussen organisaties, de commerciële waarde van het contract, de dienstverlening, de verwachtingen van afnemers, het kennisniveau, en de regulering.

Contractuele bepalingen

In contractonderhandelingen van ICT producten en diensten worden verschillende onderwerpen besproken. Voor zich sprekende onderwerpen die besproken worden zijn: aansprakelijkheid, right-to-audit, penetratietesten en wederzijdse verantwoordelijkheden. Daarnaast zijn er nog drie onderwerpen die extra context en uitleg nodig hebben omdat deze onderwerpen specifiek uit de interviews naar voren kwamen en niet strikt juridisch/contractrechtelijk zijn waardoor er wel over wordt gesproken, maar deze niet altijd in de overeenkomsten terugkomen.

1. **Assurance vragenlijsten van de afnemer -** Volwassen afnemers van IT diensten hebben vaak een eigen assurance vragenlijst waar alle leveranciers aan moeten voldoen. De kwaliteit hiervan en de standaardisatie komt volgens de leveranciers vaak niet overeen met de uitvraag van de afnemer. Daarnaast blijkt vaak dat de vragenlijsten uiteindelijk geen onderdeel vormen van het contract, maar alleen gebruikt worden als standaard procedure.

2. **Service Level Agreements (SLA) -** Als onderdeel van contracten worden vaak ook SLAs afgesloten die omschrijven wat o.a. de Recovery Point Objective (RPO) en Recovery Time Objective (RTO) zijn, binnen welke termijn de meldplicht valt, de verantwoordelijkheden van partijen, en hoe er gerapporteerd wordt. Het is niet altijd duidelijk of dit meer gedreven is vanuit performance/commercieel oogpunt of meer gedreven door informatiebeveiliging.

3. **Vereiste certificeringen -** Veel afnemers willen dat leveranciers bepaalde certificeringen hebben om aan te tonen dat ze controle hebben over hun omgeving. Veel terugkerende certificeringen en assurance verklaringen zijn ISO 27001, SOC 2 type II en ISAE 3402. Vaak worden deze certificeringen als zeer omvangrijk beschouwd (SOC 2) en is de inhoud niet altijd even helder voor betrokkenen die geen assurance/audit-achtergrond hebben. Hierdoor kan schijnveiligheid ontstaan, omdat afnemers niet begrijpen wat de certificering betekent. Daarnaast groeit het aantal mogelijke certificeringen snel en is er weinig standaardisatie.

Welk team beoordeelt de contracten?

De manier waarop contracten worden beoordeeld verschilt per team / afdeling (bijv. juridisch of cybersecurity) en per organisatie. De omvang en volwassenheid van de organisaties hebben hier mede invloed op. Afhankelijk van het team dat naar de contracten kijkt, zal de beoordeling van dergelijke contracten vanuit een ander oogpunt plaatsvinden. Dit verschil zit hem vooral in grote organisaties, bij het mkb is er vaak één verantwoordelijke persoon met een eigen achtergrond en punt waar voornamelijk op gefocust wordt in de contracten. Een selectie van betrokken teams bij het contracteerproces zijn:

Procurement - Procurement is het team wat in veel gevallen de contractonderhandelingen leidt. Specifieke kennis over cybersecurity is lang niet altijd aanwezig. Indien een partij groot genoeg is worden specifieke cyber of legal vragen doorverwezen naar andere afdelingen of personen. Een grote portie van de contracten die een “normaal” proces volgen of niet boven een bepaalde drempelwaarde uitkomen, wordt afgehandeld volgens standaard procedures of templates.

Legal - Uit de interviews blijkt dat legal vaak wordt ingeschakeld als het om specifieke juridische vraagstukken gaat, vaak gaat het hier om de aansprakelijkheidsclausules. Het verschilt per organisatie hoe legal wordt ingezet. Dit kan (bij vaak kleiner organisaties) gaan om externe inhuur, de inzet van de legal departement van de moeder organisatie of (bij grotere organisatie) de inzet van de in-house legal department.

CISO - Het CISO team zal heel erg vanuit een risk-based approach kijken naar de risico’s die gepaard gaan met een bepaalde service. De CISO wordt regelmatig betrokken bij het vaststellen van het risico profiel aan de voorkant van de uitvraag en bij specifieke cybersecurity vragen die inkoop zelf niet kan oppakken.

Security Solution Expert - Technische specialisten zullen anders naar de benodigdheden kijken. Zij zullen meer diepgang willen zien in hoe de maatregelen technisch zijn toegepast, en of deze technisch haalbaar zijn.

Deelonderwerp 2 – redenen vereisten niet opgenomen worden

Indien niet aanwezig, een omschrijving van redenen waarom contractuele vereisten niet zijn opgenomen

Bij de huidige b2b contractonderhandelingen worden cybersecurity voorwaarden niet altijd even zwaar gewogen. De belangrijkste die dit verklaren zijn: de verhoudingen, het kennisniveau, de risico's, de mogelijkheid tot beveiliging, de kosten, en de weinige geschillen die voorkomen.

De verhoudingen tussen de contracterende organisaties kunnen bepalend zijn bij de contractonderhandelingen voor het afnemen van ICT-producten en diensten (zoals besproken in deelvraag 1). Deze disbalans kan zorgen dat organisaties de onderhandelingspositie hebben om te zeggen dat wijzigingen niet gewenst zijn of geen motivatie hebben om deze toe te voegen. In het voorbeeld van een zeer grote leverancier met miljoenen afnemers is het "*take-it or leave it*' en zal er niet van de standaardvoorwaarden afgeweken worden. Ook as-a-service leveranciers hebben vaak minder ruimte voor maatwerk en hebben daardoor vaak een "*take-it or leave it*" contract liggen. Op kleinere schaal betekent deze disbalans dat het niet mogelijk is om een partnership aan te gaan, en organisaties gebonden zijn aan standaard procedures en overeenkomsten.

Het kennisniveau van de contracterende organisatie is van groot belang, om in staat te zijn de risico's en de benodigde maatregelen te identificeren (zoals besproken in deelvraag 1). In veel situaties is de kennis niet aanwezig om te weten welke vereisten goed zijn om op te nemen. Ook zijn afnemers vaak niet in staat om certificeringen juist te interpreteren, denk hierbij aan ISO 27001, SOC type II en ISAE 3402. Dit zorgt voor verkeerde aannames bij afnemers, en zorgt er ook voor dat afnemers in veel gevallen de standaard voorwaarden zullen tekenen.

Risicobeperking is de voornaamste reden om cybersecurity voorwaarden op te nemen in contracten. De omvang van die voorwaarden is sterk afhankelijk van het risico dat de contracterende organisaties lopen. Wanneer een leverancier weinig risico loopt, zijn de (aansprakelijkheids-) beperkingen in de contracten van de leverancier minder vergaand, en zullen er minder cybersecurity vereisten zijn. In het geval van hogere risico's voor de afnemers, kunnen afnemers bepaalde afspraken verkeerd interpreteren. Zo is het voor afnemers vaak niet duidelijk welke risico's ze zelf dragen, welke gezamenlijk zijn en welke bij de leverancier liggen. Soms bestaat er onterecht de verwachting dat alle risico's "afgekocht" kunnen worden en bij de leveranciers komen te liggen. Dit is een gevaarlijke misvatting (zo blijkt ook uit de jurisprudentie). Zoals geconstateerd in het theoretisch kader bevatten overeenkomsten van leveranciers vaak aansprakelijkheidsuitsluitingen. Daarnaast kunnen risico's ingeperkt worden door cybersecurity verzekeringen. In het geval van de afnemer wordt dit alleen afgesloten als de risico's te hoog zijn. Leveranciers nemen zelden een cybersecurity verzekering omdat het risico vaak te hoog is, en daardoor de kosten te hoog zijn. Ook worden de benodigdheden om verzekerbaar te zijn steeds groter. Zo hebben wij een dalende trend geconstateerd bij bedrijven die zichzelf verzekeren tegen cybersecurity incidenten. Ook is aangegeven dat de cyberaansprakelijkheid steeds meer als 'reguliere' bedrijfsaansprakelijkheid wordt gezien.

Beveiliging van de service wordt in veel gevallen ingebouwd door de leverancier. Hierbij worden onder andere bepaalde firewalls ingeregeld. Echter gaat het in veel gevallen ook om hoe de afnemer de service inricht, en welke additionele security kan worden toegevoegd. De mogelijkheid die een service biedt om cybersecuritymaatregelen toe te voegen, is van groot belang voor wat er van de leverancier verwacht wordt. Hierbij moeten de verantwoordelijkheden wel duidelijk in het contract worden opgenomen. Maar zorgt dit ervoor dat wanneer er veel ruimte is voor de afnemer om security in te bouwen er minder security vereisten voor de leverancier in de contracten zullen staan.

Kosten die gemaakt worden om een service af te nemen betekenen niet altijd dat dit de veiligere optie is. Voor veel afnemers is het moeilijk om in te schatten wat de cybersecuritystatus is van leveranciers. Hierdoor wordt soms de aanname gemaakt dat de duurdere service ook veiliger is, echter is dit niet altijd het geval. Toch zien we wel een verhoging van de kosten wanneer dit in de SLA terug te vinden is. Zo worden de kosten die door de leverancier gemaakt worden vaak direct vertaald in de kostprijs van de te leveren diensten. Zo valt er met veel leveranciers te onderhandelen over additionele maatregelen in een SLA, maar dit betekent wel dat de prijs van de te leveren diensten omhoog zal gaan. Er wordt meer maatwerk geboden en daardoor worden er dus meer kosten gemaakt.

Deelonderwerp 3 – redenen vereisten wel opgenomen worden

Indien aanwezig, omschrijving van de invulling van deze vereisten

In b2b contractonderhandelingen over cybersecurity voorwaarden zien wij grote verschillen tussen contracterende organisaties. Belangrijke verschillen zien wij vooral door de commerciële waarde van het contract, het kennisniveau, de risico's, het ontzorgen, de mogelijke reputatieschade en de regulering.

De verhoudingen tussen de contracterende organisaties kunnen bepalend zijn bij de contractonderhandelingen voor het afnemen van ICT-producten en diensten (zoals besproken in deelvraag 1). Bij gelijkwaardige verhoudingen blijkt dat er vaak behoefte is aan het aangaan van partnerships. Hierbij kunnen goede afspraken gemaakt worden over wederzijdse verantwoordelijkheden, nieuwe ontwikkelingen in de markt en verbeterplannen. Ook kan er door partnerships tussentijds bijgestuurd worden. Zo zorgt een partnership dus voor een duidelijkere definitie van de vereisten en verantwoordelijkheden.

Het kennisniveau van de contracterende organisatie is van groot belang, om in staat te zijn de risico's en de benodigde maatregelen te identificeren (zoals besproken in deelvraag 1). Volwassen organisaties hebben duidelijke vereisten die ze terug willen zien in contracten, waardoor zij altijd op basis van een risicoprofiel een leverancier zullen selecteren. Leveranciers zullen daarom aan bepaalde minimum beveiligingsvereisten moeten voldoen, als ze met grote afnemers willen contracteren.

Risicobeperking is de voornaamste reden om cybersecurity voorwaarden op te nemen in contracten. De omvang van die voorwaarden is sterk afhankelijk van het risico dat de contracterende organisaties lopen (zoals besproken in deelvraag 2).

Ontzorgen is van belang voor afnemers met een lagere volwassenheid op het gebied van cybersecurity. Die zien het liefst alle verantwoordelijkheid en maatregelen bij de leverancier liggen, omdat er intern weinig kennis aanwezig is. Dit betekent niet dat alle verantwoordelijkheid weggehaald wordt, maar wel dat de leverancier extra service biedt om de volwassenheid van de afnemer te vergroten.

Reputatie(schade) van leveranciers kan op het spel staan als een leverancier betrokken is bij een cyberincident. Dit zorgt er in sommige gevallen voor dat leveranciers meer van de zorg op zich te nemen als kwaliteitsgarantie (quality assurance) die in het voordeel is van zowel de leverancier als de afnemer.

Regulering van bepaalde organisaties zorgt voor een stimulans in het bewustzijn van de organisatie (zoals besproken in deelvraag 1). Dit leidt ook tot een versnelling van het vastleggen van afspraken wanneer sectoren gereguleerd/ gecertificeerd zijn. Dit aangezien een wettelijke verplichting of certificeringen bepaalde maatregelen vereisen (compliance-driven). Deze (gereguleerde) afspraken werken vervolgens ook verder door in de keten aangezien deze vereisten weer worden doorvertaald aan leveranciers of onderaannemers.

Hoe worden de contracten opgesteld?

Afspraken tussen leveranciers en afnemers kunnen op verschillende manieren worden vastgelegd. Belangrijke onderdelen die vaak terugkomen in de overeenkomsten zijn:

Algemene voorwaarden - Op veel standaard afspraken en overeenkomsten zullen algemene (verkoop / inkoop) voorwaarden van toepassing zijn. Uit de praktijk blijkt dat uiteindelijk de voorwaarden van de organisatie van toepassing zijn die de meeste slagkracht heeft in de onderhandelingen.

SLA – Contractuele afspraken kunnen worden aangevuld met SLAs waarin bepaalde afspraken nader zijn uitgewerkt. Deze omschrijven o.a. wat de RPO en RTO zijn, de meldtermijn, de zorgplicht en hoe en wat er gerapporteerd wordt. Vaak zijn het standaard SLAs die aan meerdere afnemers worden aangeboden, echter is er steeds meer maatwerk wat zich richt op de specifieke risico's van de afnemer.

Master Services Agreements (MSAs) - Zodra de af te nemen producten/diensten complexer of omvangrijker worden, contracteren partijen vaak niet meer op algemene voorwaarden maar zal er onderhandeld worden over een MSA. Voorwaarden van beide partijen worden dan opgenomen in een framework overeenkomst waaronder nadere opdrachten kunnen worden uitgevraagd.

Vereiste certificeringen - Veel afnemers verwachten dat leveranciers bepaalde certificeringen / assurance rapporten hebben om aan te tonen dat ze controle hebben over hun omgeving. Veel terugkerende certificeringen zijn: ISO 27001, SOC 2 type 2 en ISAE 3402. Aanvullend hierop willen afnemers vaak een *right-to-audit* afdwingen om te kunnen controleren of de leverancier aan de afspraken voldoet.

Deelonderwerp 4 – knelpunten

Omschrijving van knelpunten waar leveranciers en afnemers tegenaan lopen op gebied van cybersecurity

In b2b contractonderhandelingen over cybersecurity voorwaarden zien wij verschillende knelpunten. De belangrijkste knelpunten die wij geïdentificeerd hebben gaan over vragen rondom risicobeperking, verantwoordelijkheid, zorgplicht, veroudering, vendor lock-in, een minimale norm en eventuele geschillen.

De verhoudingen tussen de contracterende organisaties kunnen bepalend zijn bij de contractonderhandelingen voor het afnemen van ICT-producten en diensten (zoals besproken in deelvraag 1). Hier heerst het gevoel bij afnemers dat ze geen partnerships aan kunnen gaan en niet goed weten hoe ze de uitvraag moeten formuleren, afspraken lijken vaak puur sales gedreven. Leveranciers merken op dat er door de kennis achterstand de verkeerde uitvraag wordt gedaan of dat er enkel checklists worden verstuurd als onderdeel van een standaard procedure.

Het kennisniveau van de contracterende organisatie is van groot belang, om in staat te zijn de risico's en de benodigde maatregelen te identificeren (zoals besproken in deelvraag 1). Er zijn weinig standaardmaatregelen en kaders voor organisaties die niet gereguleerd worden of onder een bepaalde brancheorganisatie vallen. Daarnaast is cybersecurity vaak geen kerntaak bij mkb bedrijven en hebben ze ook niet de juiste expertise in dienst, hierdoor worden de meeste maatregelen ad-hoc genomen.

Risicobeperking is de voornaamste reden om cybersecurity voorwaarden op te nemen in contracten. De omvang van die voorwaarden is sterk afhankelijk van het risico dat de contracterende organisaties lopen (zoals besproken in deelvraag 2). Zo zullen additionele maatregelen wenselijk zijn wanneer risico's en daardoor de cybervereisten van de afnemer groter zijn dan de standaard maatregelen van de leverancier.

Verantwoordelijkheden in het geval van een incident moeten goed gedefinieerd worden. Wie is verantwoordelijk voor welke stap in het proces en de reactie op een incident? We zien bij volwassen organisaties dat hier uitgebreid over onderhandeld wordt en dat incidenten ook periodiek getest worden door middel van use cases. Bij minder volwassen organisaties zien wij juist vaak dat deze verantwoordelijkheden niet helemaal duidelijk zijn en soms onterecht wordt gedacht dat verantwoordelijkheden volledig bij de leverancier liggen.

Zorgplicht is een onderwerp dat bij veel organisaties speelt maar grote verschillen kent in de uitvoering. Zo is een leverancier van een dienst aan veelal kritieke mkb afnemers zich heel erg bewust dat er zorg nodig is om de dienst veilig te gebruiken. In een sterk gereguleerde sector zijn de (wettelijke) kaders vaak al duidelijker en is ook de zorgplicht duidelijker omkaderd. De zorg die er geleverd wordt verschilt dan ook significant tussen organisaties.

Veroudering van contracten zorgt voor grote risico's bij afnemers. Nieuwe contracten worden vaak wel herzien en met steeds meer oog voor cybersecurity afgenomen. Oudere / langlopende contracten zijn niet eenvoudig 'open te breken' om er nieuwe / aanvullende (cybersecurity) vereisten in op te nemen. Daarnaast worden er in de praktijk niet voldoende periodieke risicoanalyses, penetratietesten en audits gedaan om de kwaliteit te blijven garanderen.

Vendor lock-in is een fenomeen wat ervoor zorgt dat afnemers toch bij de bestaande leverancier blijven. Dit komt voor wanneer een afnemer een hoge afhankelijkheid heeft van de diensten en hoge kosten zou moeten maken om te wisselen van leverancier.

Ontbreken van minimale norm van vastlegging voor relatief kleine organisaties c.q. standaardisatie voor relatief kleine organisaties. Leveranciers krijgen op hun beurt weer te maken met zware administratieve lasten in de vorm van uiteenlopende vragenlijst van diverse afnemers.

Hoe worden (eventuele) geschillen opgelost?
In het geval van een geschil is er vaak een standaard procedure die start (verbeter protocollen en escalatie procedures). De intentie van de leveranciers en afnemers is om er door middel van goede afspraken met elkaar uit te komen. De weg naar de rechter wordt dus niet snel gezocht. Daarnaast kan er ook sprake zijn van vendor lock-in waardoor overstappen (vooral voor afnemers) lastig en prijzig blijkt. Hierdoor wordt er vaak een verbeterplan opgesteld om de dienst te verbeteren en het risico op herhaling te beperken. Alleen als er grote schendingen zijn van contractuele afspraken zal er naar de rechter gestapt worden.

Deelonderwerp 5 – mogelijke beleidsinstrumenten

Overzicht van mogelijke (beleids-)instrumenten en relevante prikkels voor het stimuleren van heldere contractuele afspraken op het gebied van cybersecurity

In b2b contractonderhandelingen over cybersecurity voorwaarden zien wij grote verschillen bij verschillende organisaties. Mogelijke beleidsinstrumenten die ingezet kunnen worden om de volwassenheid van organisaties op te krikken richten zich op harmonisatie, wet- en regelgeving en overheidssteun.

Harmonisatie en standaardisatie wordt door veel organisaties genoemd als een wenselijke ontwikkeling. Dit komt doordat organisaties aan steeds meer verschillende eisen moeten voldoen. Als organisaties ook internationaal handelen wordt deze eisenlijst nog groter. Documentatie waarin begrijpelijke kaders worden gegeven, minimum eisen in worden geïntegreerd en bijvoorbeeld template contracten worden aangeboden zijn daarom wenselijk.

Harmonisatie kan gestimuleerd worden in sectoren en samenwerkingsverbanden waar dezelfde belangen spelen. Dit zal leiden tot meer onderhandelingskracht voor kleinere organisaties. Op die manier kunnen relevante eisen in de contracten opgenomen worden. Er komt veel (nieuwe) wet- en regelgeving op organisaties af o.a. NIS2, DORA en de CRA. Standaardisatie van deze wetgeving zit hem in het bieden van kaders waarin de verschillende richtlijnen geïntegreerd worden. Dit kan door het ontwikkelen van begrijpelijke toelichtingen, handelingskaders en standaardcontracten die de verschillende wetten integreren.

Op verschillende niveaus wordt standaardisatie gewenst. Zo zou een bepaalde mate van standaardisatie in transparantie van leveranciers over hun cybersecurity status gewenst zijn. Zo worden leveranciers makkelijker te auditen en wordt het makkelijker om de security status van een leverancier te kunnen beoordelen (kosten hiervoor zijn wel voor de afnemer), dit is in sommige gevallen wenselijk wanneer een leverancier niet over een certificering beschikt.

Daarnaast zouden standaard kaders over de zorgplicht van leveranciers helpen om de verantwoordelijkheden duidelijker te krijgen. Ook zou er meer duidelijkheid gegeven moeten worden over welke certificeringen leidend zijn en een goede weerspiegeling geven van de huidige cybersecurity status. Dit is wenselijk om de verschillende certificaten (o.a. ISO, SOCII en ISAE) te begrijpen, toe te passen en af te dwingen. Dit biedt meer richting voor kleinere bedrijven om vertrouwen te kweken. Nu is er veel vertrouwen in grote leveranciers, bij kleine leveranciers is dit vertrouwen minder en is er meer behoefte aan het uitvoeren van o.a. penetratietesten.

Nadere kaders/toelichting voor regelgeving worden nodig geacht om beter tot de kern van cyberveiligheid te komen. Kaders en toelichting zouden bijvoorbeeld meer duidelijkheid moeten geven over waar de verantwoordelijkheid van de leverancier stopt en waar de verantwoordelijkheid van de afnemer begint. Ook als het gaat om zorgplicht kan hier meer duidelijkheid op komen. Hierbij is er behoefte aan begrijpelijke uitleg van bestaande en nog te ontwikkelen regelgeving met bijvoorbeeld bepaalde casuïstiek/praktijkvoorbeelden. De NCSC- en DNB richtlijnen geven hiervoor een goed voorbeeld. Leg hierbij de nadruk op Cloud, aangezien 90% van de dienstverlening zich tegenwoordig richt op Cloud.

Overheidssteun wordt niet altijd gevoeld door organisaties. Organisaties die gereguleerd zijn, onderdeel uitmaken van een brancheverenigingof een krachtige Private Equity- of moedermaatschappij hebben minder steun nodig. Overige (mkb) organisaties hebben echter meer hulp en concrete kaders over het toepassen van cybersecurity in de organisatie nodig. Om deze reden moet de steun niet alleen gericht zijn op contracten, maar op het ondersteunen van de gehele cyberveiligheid van de organisatie. Overheidssteun kan gegeven worden op verschillende manieren:

- **Bewustzijn -** Organisaties en werknemers zijn zich vaak niet bewust van de digitale risico's. Leveranciers merken ook dat door kleine afnemers weinig naar cyber gevraagd wordt. Hierdoor is het van belang om meer te onderwijzen. Platformen als NCSC en Digital Trust Center worden wel gewaardeerd, maar niet breed gebruikt. Het is voor organisaties niet altijd duidelijk naar welk loket men toe kan voor welke vraag.
- **Zorgplicht –** Wordt tot in bepaalde mate in de contracten opgenomen door de leveranciers. De overheid kan hier echter wel een actievere rol in spelen, bijvoorbeeld door het definiëren van best-practices en minimum benodigdheden / vereisten.
- **Vangnet -** Een organisatie heeft geen sociaal vangnet vanuit de overheid in het geval van cyberincidenten. Wanneer er fysieke schade wordt geleden door een bedrijf zal er ondersteuning zijn van de politie. In het geval van digitale schade is er in veel mindere mate een vangnet. Het is belangrijk dat organisatie weten waar en bij wie ze terecht kunnen voor hulp, kaders en documentatie. Nu weten organisaties dit niet altijd te vinden. Denk hierbij aan een centraal platform of centraal contactpunt.

5

Belangrijkste adviezen

Belangrijkste adviezen

Een omschrijving van de belangrijkste adviezen

Onze belangrijkste adviezen en vervolgstappen zijn gebaseerd op een combinatie van inzichten. Deze inzichten zijn verkregen uit de interviews, onze eigen ervaring en de bijbehorende kronieken. In de praktijk zien wij dat contractuele afspraken vaak niet doorslaggevend zijn om met een organisatie in zee te gaan. Daarnaast wordt er ook weinig teruggegrepen op de contractuele afspraken in het geval van incidenten. In veel grotere mate gaat het om het vertrouwen dat de organisatie heeft in de capaciteiten van de andere organisatie en de meerwaarde van de service die geboden wordt. Om deze reden is onze voornaamste afdronk dat het belangrijker is om organisaties te helpen om hun cybersecurity preventief beter in te regelen, dan om dit juridisch af te vangen. Onderdeel van het beter inregelen van cybersecurity is wel degelijk het toepassen van een minimale norm in contracten. Echter is het daarnaast ook van belang om sturing te geven op beoordelen van de risico's van de service en de capaciteiten van de organisatie. Onze belangrijkste adviezen zijn dan ook als volgt:

Deel informatie over best practices

Zorg voor een centrale plek waar duidelijke en concrete voorbeelden worden gegeven van best practices in de markt om cybersecurity te verbeteren. Communiceer dit middel naar de markt als de centrale plek voor alle hulp die het ministerie biedt rondom cybersecurity. Leg de focus binnen dit platform op het vergroten van het bewustzijn, de concrete te nemen technische maatregelen en minimale voorwaarden om in contracten op te nemen. Zorg hierbij ook dat er aandacht wordt besteed om het volwassenheidsniveau meetbaar te maken aan de hand van concrete kaders.

Standaardiseer en maak kaders beschikbaar voor regelgeving

Stuur aan op het belang van standaardisering en harmonisatie. Hierbij worden duidelijke kaders verwacht voor wet- en regelgeving rondom contractuele afspraken, waarbij zo veel mogelijk harmonisatie bestaat tussen verschillende binnen- en buitenlandse regels. De huidige wetgeving kent een hoop overlap, echter zit er in de aanpak tot compliance weinig integratie van de verschillende wetgevingen. Hierbij is meer toelichting nodig op wet- en regelgeving in duidelijk taal met praktijk voorbeelden, stadaard kaders en templates. Ook moet de waarde van een certificering voor een afnemer verbeteren, de baten voor de afnemers moeten duidelijk zijn en voor afnemers moet begrijpelijke toelichting op certificering beschikbaar zijn om certificeringseisen ook daadwerkelijk te begrijpen en de juiste vragen aan leveranciers te kunnen stellen. Er moet voorkomen worden dat met name de mkb leverancier gaan bezwijken onder de druk van afnemers die allemaal met eigen eisen, wensen, vragenlijsten en auditverzoeken komen. Daar is ook en verdiepingsslag van de certificeringen voor nodig om meer zekerheid te krijgen op het volwassenheidsniveau van de organisatie.

Biedt financiële prikkel/ondersteuning

Creëer een sociaal vangnet waar organisaties terecht kunnen wanneer zij ernstige digitale schade lijden. Denk hierbij aan een centraal platform of centraal contact punt. Begeleid organisaties in het nemen van vervolgstappen om te herstellen van de schade. Leg hierbij de nadruk op juridisch te nemen stappen om alle benodigde belanghebbende juist te informeren.

6

Volgende stappen

Volgende stappen

Een omschrijving van de stappen die wij adviseren als vervolg op dit onderzoek

Het doel van de belangrijkste adviezen is ook om volgende stappen te activeren. Op basis van onze eigen ervaring identificeren wij de onderstaande stappen als een mogelijk stappenplan dat uitgevoerd kan gaan worden.

Stap 1: Cybersecurity platform
Richt een online platform in om organisaties te bereiken en te helpen om hun digitale weerbaarheid te versterken. Zorg voor veel zichtbaarheid en bekendheid voor dit platform (bijvoorbeeld via NCSC en MKB-Nederland). Het platform moet een plek bieden waar organisaties terecht kunnen voor al hun vragen omtrent cybersecurity. Zorg ervoor dat dit platform breed gedeeld wordt en zich hoofdzakelijk richt op de bijbehorende risico's, praktische acties en voorbeelden die voor iedere organisatie van belang zijn en het begrijpelijk maken van de verwachtingen van organisaties.

Stap 2: Awareness modules
Creëer awareness modules (rondom verschillende cybersecurity onderwerpen met o.a. cybersecurity vereisten in contracten en veranderende en nieuwe wet-en regelgeving) en biedt deze aan op het online platform. Geef hierbij op instap niveau aan wat de belangrijkste stappen zijn om te nemen en wat ook mogelijke vervolgstappen zijn om nog meer risico's te beperken.

Stap 3: Meetmethode voor cyberniveau
Creëer een methode die organisaties in staat stelt om hun eigen cyberniveau te kunnen meten. Geef hierbij als output bepaalde richtlijnen voor de te nemen stappen om verder te ontwikkeling in cybervolwassenheid.

Stap 4: Contract templates
Creëer contract templates om houvast te bieden aan ondernemers met weinig interne expertise. Zorg hierbij dat verschillende wetten geïntegreerd worden. Daarbij is het van belang dat aangetoond wordt waar rekening mee gehouden moet worden in welke regelgeving.

Stap 5: Ontwikkel toelichtingen op regelgeving
Ontwikkel toelichtingen op huidige en nieuwe wetgeving in begrijpelijke taal en aan de hand van praktijk voorbeelden. Ontwikkel kaders die het begrip van en verhouding tussen verschillende internationale, nationale en regionale regelgeving duidt. Dit kan op een platform (stap 1) of via brochures.

Stap 6: Harmonisatie certificeringen
Harmoniseer certificeringen, doe dit door een vertaalslag te maken tussen de verschillende certificeringen. Geef hierbij duidelijk aan wat de overeenkomsten en verschillen zijn. Zorg daarbij ook dat er duidelijkheid gegeven wordt op certificeringen die het meest inzicht geven in de controle van bepaalde cyberrisico's. Leg hierbij nadruk op welke certificeringen het meest voor de hand liggen in bepaalde sectoren en bij het behandelen van bepaalde persoonsgegevens.

Stap 7: Sociaal vangnet
Creëer een sociaal vangnet (bijvoorbeeld in de vorm van een platform (stap 1) of centraal contactpunt) waar organisaties terecht kunnen wanneer zij (ernstige) digitale schade lijden. Begeleid organisaties in het nemen van vervolgstappen om te herstellen van de schade. Leg hierbij de nadruk op juridisch te nemen stappen om alle benodigde belanghebbende juist te informeren.

Stap 8: Harmonisatie cybersecurityverzekeringen
Hou meer toezicht op cybersecurityverzekeringen, creëer standaard regels die organisaties in staat stelt om verzekerbaar te zijn. Nu is dit een uitgebreid proces vol met vragenlijsten en beoordelingen die nodig zijn om überhaupt verzekerd te kunnen worden. Daarnaast moet er duidelijk aangegeven worden wat er verzekerd wordt en waar de verantwoordelijkheden liggen.

A

Appendix

A.1: Onderbouwing van de onderzoeksmatrix

De matrices in de volgende slides bevat twee assen: de sector en de omvang van de organisatie. De onderbouwing voor de keuze en verdeling van deze assen wordt hier besproken.

Classificatie sectoren afnemers

De onderzoeksmatrix bevat 22 verschillende sectoren. Deze sectoren zijn gedefinieerd door de Europese Commissie in de ‘statistical classification of economic activities’.[1]

A AGRICULTURE, FORESTRY AND FISHING (en)
B MINING AND QUARRYING (en)
C MANUFACTURING (en)
D ELECTRICITY, GAS, STEAM AND AIR CONDITIONING SUPPLY (en)
E WATER SUPPLY; SEWERAGE, WASTE MANAGEMENT AND REMEDIATION ACTIVITIES (en)
F CONSTRUCTION (en)
G WHOLESALE AND RETAIL TRADE (en)
H TRANSPORTATION AND STORAGE (en)
I ACCOMMODATION AND FOOD SERVICE ACTIVITIES (en)
J PUBLISHING, BROADCASTING, AND CONTENT PRODUCTION AND DISTRIBUTION ACTIVITIES (en)
K TELECOMMUNICATION, COMPUTER PROGRAMMING, CONSULTING, COMPUTING INFRASTRUCTURE AND OTHER INFORMATION SERVICE ACTIVITIES (en)
L FINANCIAL AND INSURANCE ACTIVITIES (en)
M REAL ESTATE ACTIVITIES (en)
N PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES (en)
O ADMINISTRATIVE AND SUPPORT SERVICE ACTIVITIES (en)
P PUBLIC ADMINISTRATION AND DEFENCE; COMPULSORY SOCIAL SECURITY (en)
Q EDUCATION (en)
R HUMAN HEALTH AND SOCIAL WORK ACTIVITIES (en)
S ARTS, SPORTS AND RECREATION (en)
T OTHER SERVICE ACTIVITIES (en)
U ACTIVITIES OF HOUSEHOLDS AS EMPLOYERS AND UNDIFFERENTIATED GOODS - AND SERVICE-PRODUCING ACTIVITIES OF HOUSEHOLDS FOR OWN USE (en)
V ACTIVITIES OF EXTRATERRITORIAL ORGANISATIONS AND BODIES (en)

Classificatie sectoren leveranciers

De onderzoeksmatrix bevat 11 verschillende ICT sectoren. Deze sectoren zijn gedefinieerd door de Europese Commissie in de ‘statistical classification of economic activities’.[1]

ICT sector	ICT Manufacturing	Manufacture of electronic components and boards
		Manufacture of computers and peripheral equipment
		Manufacture of communication equipment
		Manufacture of consumer electronics
		Manufacture of magnetic and optical media
	ICT Services	Wholesale of information and communication equipment
		Software publishing
		Telecommunications
		Computer programming, consultancy and related activities
		Data processing, hosting and related activities; web portals
		Repair of computers and communication equipment

1 Statistical Classification of Economic Activities in the European Community, Rev. 2.1 (NACE Rev. 2.1)

A.2: Onderbouwing van de onderzoeksmatrix

Omvang organisaties

De onderzoeksmatrix bevat 4 verschillende categorieën voor de omvang van ondernemingen. Deze categorieën zijn gedefinieerd door de Europese Commissie.[1] In dit onderzoek wordt een onderneming als groot bestempeld wanneer deze groter is dan de middelgrote onderneming.

Categorie onderneming	Aantal werkzame personen	Omzet	of	Balanstotaal
Groot	≥ 250	> € 50 m		> € 43 m
Middelgroot	< 250	≤ € 50 m		≤ € 43 m
Klein	< 50	≤ € 10 m		≤ € 10 m
Micro	< 10	≤ € 2 m		≤ € 2 m

1 Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (Voor de EER relevante tekst) (kennisgeving geschied onder nummer C(2003) 1422)

A.3: Interviews: Onderzoeksmatrix Afnemers

In onderstaande tabel is onze selectie van afnemers geïllustreerd. Hierbij hebben wij de afnemers verdeeld op basis van de sector waar zij zich in bevinden en de omvang van de organisatie.

	Agriculture	Mining & Quarrying	Manufacturing	Electricity supply	Water supply	Construction	Wholesale and retail	Transportation	Accomodation and food services	Publishing and broadcasting	Telecommunication	Financial and Insurance	Real estate	Professional, scientific and technical	Administrative and support services	Public administration	Education	Human health and social work	Arts, sports and recreation	Other services	Activities of households	Activities of extraterritorial
Grote bedrijven			I					I		I								I				
Middelgrote bedrijven												I							I			
Kleine bedrijven														I	I							
Micro bedrijven																						

- In bovenstaande tabel zijn de geïnterviewde afnemers geplot.
- ‘I’ -> betekent dat een organisatie is gesproken (met weergave van de omvang in de rij en in de kolom de sector).
- Een grijs vak betekent dat deze buiten de scope van dit onderzoek viel, en donker oranje dat deze sector geïnterviewd is.

A.4: Interviews: Onderzoeksmatrix Leveranciers

In onderstaande tabel is onze selectie van leveranciers geïllustreerd. Hierbij hebben wij de leveranciers verdeeld op basis van de sector waar zij zich in bevinden en de omvang van de organisatie.

	ICT sector										
	ICT manufacturing					ICT Services					
	Manufacture of electronic components and boards	Manufacture of computers and peripheral equipment	Manufacture of communication equipment	Manufacture of consumer electronics	Manufacture of magnetic and optical media	Wholesale of information and communication equipment	Software publishing	Telecommunications	Computer programming, consultancy and related activities	Data processing, hosting and related activities; web portals	Repair of computers and communication equipment
Grote bedrijven							I		I	I	
Middelgrote bedrijven									I	I	
Kleine bedrijven							I			I	
Micro bedrijven											

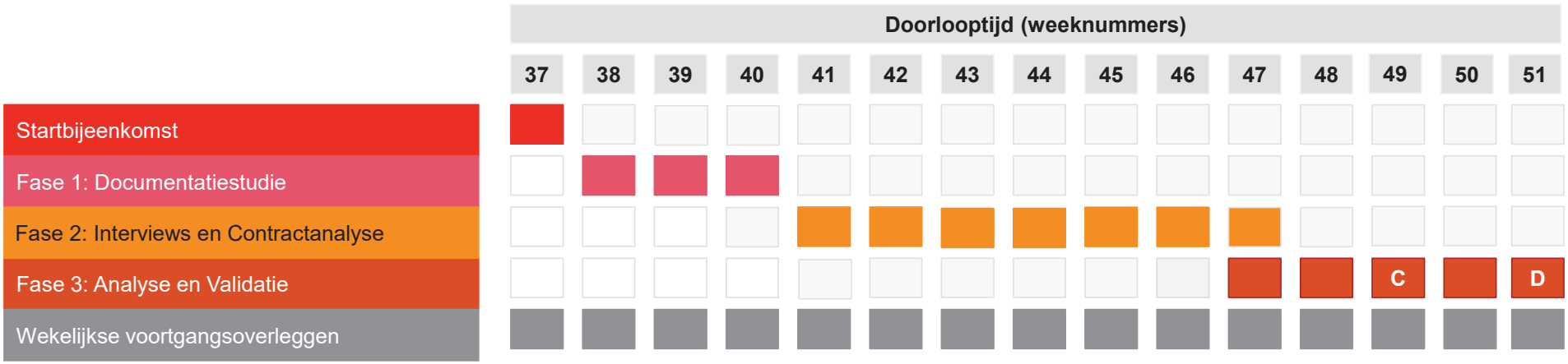
- In bovenstaande tabel zijn de geïnterviewde leveranciers geplot.
- 'I' -> betekent dat een organisatie is gesproken (met weergave van de omvang in de rij en in de kolom de sector).
- Een grijs vak betekent dat deze buiten de scope van dit onderzoek viel, en donker oranje dat deze sector geïnterviewd is.

*Tot slot is het van belang om een nuance aan te brengen op de leverancier/afnemer verhoudingen. Zo zijn leveranciers vaak ook afnemers. Wij hebben deze organisaties tijdens de interviews benaderd vanuit hun rol als leverancier.

B: Planning

De start van het onderzoek was in week 37 van 2023, de oplevering van de definitieve rapportage is op 21 december 2023.

- In de wekelijkse voortgang overleggen is de planning besproken en waar nodig aangepast.
- Concept rapportage (C), Definitief rapport (D).



C: Gebruikte documentatie

Een literatuurlijst van de documentatie die is beoordeeld.

Bron	Documentatie
Bestaande rapporten over onderwerp	Nederlandse cybersecuritystrategie 2022 - 2028 De Nederlandse Cybersecuritystrategie (NLCS) is tot stand gekomen met een brede betrokkenheid van publieke, private en maatschappelijke organisaties, onder coördinatie van de NCTV. Het Cybersecuritybeeld Nederland 2022 (CSBN) vormt het uitgangspunt voor de pijlers en doelstellingen van de NLCS.
	ENISA: Good practices for supply chain cybersecurity The European Union Agency for Cybersecurity (ENISA), *Good Practices for Supply Chain Cybersecurity*, 2023
	Aansprakelijkheid voor digitale onveiligheid in b2b-relaties B. Nieuwesteeg, M. Faure en L. Visscher, *Studie: Aansprakelijkheid voor digitale onveiligheid in b2b-relaties,* 2020.
Wet- en regelgeving (Europees)	Cyber Resilience Act Voorstel voor een Verordening van het Europees Parlement en de Raad van 15 september 2022 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020, *COM(2022) 454.*
	EU Cybersecurity Act Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening).
	Radio Equipment Directive Richtlijn (EU) 2014/53 van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG.

C: Gebruikte documentatie

Een literatuurlijst van de documentatie die is beoordeeld.

Bron	Documentatie
Wet- en regelgeving (Europees)	NIS2 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).
	Algemene Verordening Gegevensbescherming Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
Wet- en regelgeving (nationaal)	Burgerlijk Wetboek
Jurisprudentie	Rb. Overijssel, 10 mei 2023, ECLI:NL:RBOVE:2023:1731.
	Hof Amsterdam, 14 juli 2020, ECLI:NL:GHAMS:2020:2016.
	Hof Amsterdam, 7 juli 2020, ECLI:NL:GHAMS:2020:1987.
NLdigital	NLdigital voorwaarden Zoals beschikbaar gesteld op de website van NLdigital.
Kronieken	E. van Genuchten, R. van Schaik en R. Westerdijk, 'Kroniek IT-Recht 2020', *Adv. bl.* 2021, afl. 3, p. 57-64.
	V. van Druenen, E. van Genuchten en R. van Schaik, 'Kroniek IT-Recht 2021', *Adv. bl.* 2022, afl. 3, p. 71-81.
	V. van Druenen, R. van Schaik en W. Weijland, 'Kroniek IT-Recht 2022', *Adv. bl.* 2023, afl. 3, p. 79-88.