Deloitte.

Cyberweerbaarheidskloof

Aanbevelingen voor een cyberweerbaar mkb en het verkleinen van de cyberweerbaarheidskloof in Nederland

26 april 2024 | Afbeelding AI gegenereerd

Inhoudsopgave

Figurenlijst

Tabellenlijst

Samenvatting

Samenvatting

Dit onderzoeksrapport, opgesteld in opdracht van de Cyber Security Raad[1], heeft als doel strategische aanbevelingen aan te dragen, die bijdragen aan het **versterken van de cyberweerbaarheid van zelfstandigen zonder personeel (zzp) en het midden- en kleinbedrijf (mkb)** (1-249 medewerkers; hierna gezamenlijk 'het mkb'). De inzichten en conclusies zijn gebaseerd op literatuuronderzoek en directe gesprekken met: 32 mkb'ers, de klankbordgroep, aanbieders van hulpmiddelen en Deloitte experts uit het buitenland.

Nederland is onvoldoende weerbaar tegen digitale dreigingen, waarbij er grote verschillen zijn in de cyberweerbaarheid tussen organisaties[2]. Deze verschillen duiden op een cyberweerbaarheidskloof tussen 'voorlopers' die succesvol cyberrisico's en afhankelijkheden kunnen inschatten en de weerbaarheid van hun organisatie hierop kunnen aanpassen, en 'achterblijvers' die hier onvoldoende in slagen. Vooral **het mkb is hier kwetsbaar**. Deze bedrijven, met een kleiner aantal werknemers, voeren gemiddeld genomen minder vaak een risicoanalyse uit en implementeren minder ICT-veiligheidsmaatregelen[3,4]. Deze digitale kwetsbaarheid vormt een risico voor de gehele samenleving, gezien het **grote maatschappelijke en economische belang van de ruim 2 miljoen zzp'ers en mkb'ers.** Gezamenlijk genereren ze aanzienlijke werkgelegenheid, spelen ze een belangrijke rol in het Nederlandse innovatie- en concurrentievermogen, en dragen ze bij aan regionale ontwikkeling en sociale cohesie. In een tijdperk waarin organisaties digitaliseren en in toenemende mate onderling verbonden zijn in waardeketens, is het daarom essentieel dat het mkb het vermogen heeft om (relevante) **digitale risico's te verminderen tot een aanvaardbaar niveau,** zeker gezien het continu veranderende dreigingslandschap. Om de nationale cyberweerbaarheid te versterken en de cyberweerbaarheidskloof te verkleinen, dient Nederland over de gehele linie te beschikken over cybervolwassen organisaties. Dit betekent dat zowel de overheid als het mkb verantwoordelijk zijn voor het verbeteren van de cyberweerbaarheid van onze samenleving, om te zorgen dat ons land open, veilig en welvarend blijft.

Bedrijven binnen het mkb ervaren obstakels in het verhogen van hun huidige cyberweerbaarheidsniveau naar een **optimaal niveau, passend bij het risicoprofiel** van het bedrijf. Er zijn acht obstakels geïdentificeerd, waarbij geïnterviewde mkb'ers aangeven vooral moeite te hebben met de eerste drie obstakels; zie hieronder. Gezamenlijk worden deze 3 obstakels ruim zes keer zo vaak genoemd vergeleken met het totaal van obstakels 4-8.

1. **Onvoldoende cyberbewustzijn en -kennis.** Dit obstakel wordt door 84% van de in totaal 32 geïnterviewde bedrijven genoemd, en vormt het fundament voor obstakel 2 en 3 gezien de samenhang en volgordelijkheid tussen deze obstakels. Hulp vanuit de overheid voor dit obstakel is niet specifiek toegespitst op bedrijven binnen het mkb, bepaalde sectoren of het type bedrijf. Geïnterviewden geven aan überhaupt niet of beperkt bekend te zijn met partijen zoals het DTC[5] en NCSC[6], en de hulp die ze bieden. Mkb'ers zien wel een duidelijke coördinerende, faciliterende en verbindende rol voor de overheid in het communiceren en benadrukken van het belang en de urgentie van cyberweerbaarheid.
2. **Onvoldoende inzicht in risico's en handelingsperspectief.** Slechts 55% van de geïnterviewden geeft aan een risicoanalyse te hebben uitgevoerd; dit terwijl er wel een sterke behoefte is voor concreet handelingsperspectief dat is gebaseerd op het risicoprofiel van het bedrijf. Met 72% van de in totaal 39 geïdentificeerde publieke hulpmiddelen, aangeboden vanuit 10 verschillende partijen, concentreert de hulp vanuit de overheid zich op het bieden van handelingsperspectief. Slechts een klein deel van deze hulpmiddelen levert maatwerk, en het gehele aanbod van hulpmiddelen, zowel publiek als privaat, is onoverzichtelijk en onsamenhangend. De twee publieke hulpmiddelen voor het creëren van inzicht in risico's zijn beperkt in diepgang, zijn onvoldoende gekoppeld aan het individuele risicoprofiel en bieden beperkte maatregelen voor het versterken van het cyberweerbaarheidsniveau.
3. **Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden.** De kern van dit obstakel is de vraag: "wanneer is goed, goed genoeg?". Geïnterviewden geven aan dat het versterken van de cyberweerbaarheid hun eigen verantwoordelijkheid is, en dat ze bereid zijn hierin te investeren zolang ze weten waarin ze investeren, en in hoeverre het de risico's afdekt. Hierin ligt een sterke koppeling met obstakel 2 gezien de noodzaak voor het creëren van inzicht in risico's. Vanuit de overheid zijn geen hulpmiddelen gevonden voor het inschatten van de hoogte van de benodigde investeringen, of het selecteren van passende cyberweerbaarheidsmaatregelen. In het verlengde hiervan geven geïnterviewde mkb'ers aan moeite te hebben met het selecteren van en samenwerken met ICT-dienstverleners. Hier zijn enkele hulpmiddelen voor, waaronder een Checklist Service Level Agreement van het DTC[7] en het CCV keurmerk voor ICT-dienstverleners[8] (in ontwikkeling).

Obstakels 4-8 zijn, in tegenstelling tot 1-3, externe obstakels. Bedrijven binnen het mkb hebben niet direct invloed op deze obstakels.

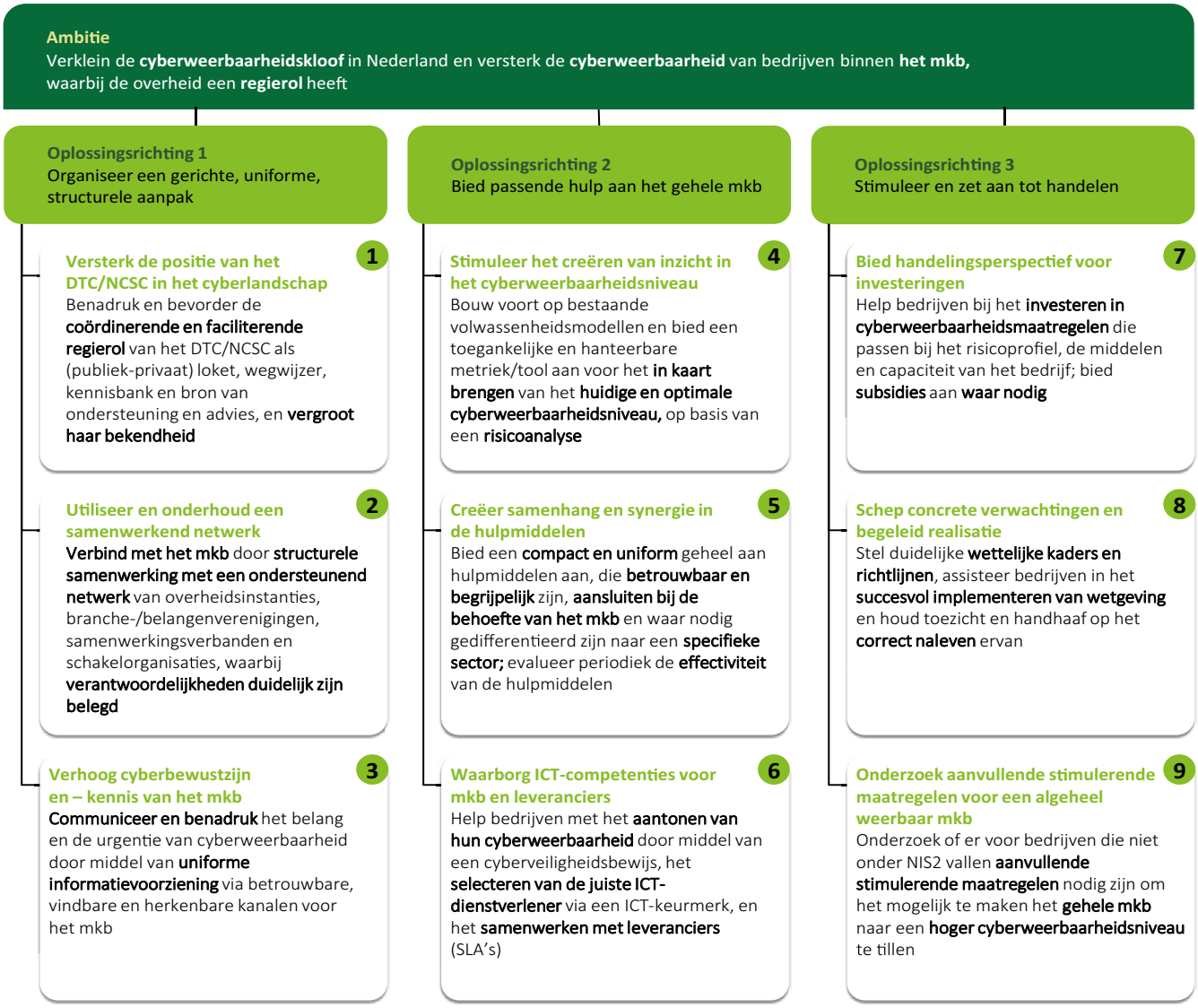
1 Voor meer informatie zie https://www.cybersecurityraad.nl/
2 Cybersecuritybeeld Nederland 2021 & 2022, Nationaal Coördinator Terrorismebestrijding en Veiligheid
3 "Veel kleine bedrijven zijn onvoldoende cyberweerbaar", Digital Trust Center webpagina, 22 mei 2023
4 Cybersecuritymonitor 2022, Centraal Bureau voor de Statistiek
5 Digital Trust Center, organisatie opgericht in 2018 door het ministerie van Economische Zaken en Klimaat ter ondersteuning van Nederlandse bedrijven in veilig digitaal ondernemen
6 Nationaal Cyber Security Centrum, onderdeel van het ministerie van Justitie en Veiligheid en verantwoordelijk voor het bevorderen van de digitale veiligheid in Nederland
7 Zie "Afspraken maken met een IT-leverancier" van het Digital Trust Center
8 Zie "Minister wil cybersecurity-keurmerk om mkb te helpen" van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), 2 oktober 2023

4. Algemeen tekort aan personeel in Nederland met expertise in ICT en cyberveiligheid;
5. Beperkte toepasbaarheid huidige cyberrichtlijnen voor het mkb;
6. Afhankelijkheidsrisico's in toeleveringsketen;
7. Beperkte vindbaarheid van (overheids-)hulpmiddelen;
8. Veranderend dreigingslandschap.

Voortkomend uit een analyse van de obstakels, hulpmiddelen en behoeftes, zijn er **negen strategische aanbevelingen opgesteld** (zie Figuur 1) die de overheid richting geven in de aanpak om de cyberweerbaarheidskloof in Nederland te verkleinen, door bedrijven binnen het mkb te helpen met het versterken van hun cyberweerbaarheid. De strategische aanbevelingen zijn onderverdeeld in drie oplossingsrichtingen:

1. **Organiseer een gerichte, uniforme, structurele aanpak.** Deze oplossingsrichting richt zich op het netwerk van partijen in het cyberlandschap en hun onderlinge verbinding.
2. **Bied passende hulp aan het gehele mkb.** Deze oplossingsrichting richt zich op het doen aansluiten van de hulp vanuit de overheid op de behoefte van het mkb.
3. **Stimuleer en zet aan tot handelen.** Deze oplossingsrichting richt zich op het activeren van bedrijven zodat ze stappen zetten in het versterken van hun eigen cyberweerbaarheid.

Voor dit alles is een samenwerkend netwerk nodig met publiek-private partners dat in directe verbinding staat met het mkb. Binnen het netwerk zijn de rollen en verantwoordelijkheden duidelijk gedefinieerd. Een effectieve aanpak voor het versterken van de cyberweerbaarheid van het mkb vereist een combinatie van overheidsinitiatieven en marktoplossingen. De markt kan bijdragen met innovatie, toegang tot de nieuwste technologieën, en heldere (contractuele) afspraken met afnemers van hun diensten. De overheid kan kaders stellen, regelgeving ontwikkelen en implementeren en een regierol vervullen. Voor alle strategische aanbevelingen geldt dat er naar landen als Denemarken en het Verenigd Koninkrijk gekeken kan worden voor inspiratie en werkzame oplossingen, waarbij onderzoek nodig is naar 'best practices' en de toepasbaarheid in de Nederlandse context.



Figuur 1 Strategische aanbevelingen, onderverdeeld in oplossingsrichtingen

1. Introductie

1. Introductie

1.1 Achtergrond

In een tijdperk waarin digitale verbondenheid essentieel is voor onze samenleving, staat cyberveiligheid hoog op zowel de Europese als nationale agenda. De Nederlandse overheid heeft in 2023 de Nederlandse Cybersecuritystrategie (NLCS) gepubliceerd, evenals structurele middelen vrijgemaakt die specifiek gericht zijn op het verhogen van de digitale weerbaarheid[9]. De overheid neemt daarmee meer regie dan voorheen en gaat centraal organiseren waar dat kan, zonder de eigen verantwoordelijkheid voor cyberveiligheid weg te nemen bij de bedrijven. Bedrijven zullen meer en meer (wettelijk) ertoe worden aangezet om hun eigen cyberweerbaarheid te versterken en om te investeren in het beveiligen van de digitale producten en diensten die zij aanbieden. Dit zal ook onder de druk van nieuwe Europese wetgeving toenemen[10].

Cyberveiligheid omvat alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of te herstellen als er schade is. Voorbeelden van schade zijn dat men niet meer gebruik kan maken van een computersysteem wanneer men dat wil of dat de opgeslagen informatie bij anderen terecht komt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen. Cyberweerbaarheid is het vermogen om (relevante) digitale risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken[11].

Bij een groot aantal bedrijven is er al aandacht voor het implementeren van cyberveiligheidsmaatregelen om de cyberweerbaarheid te waarborgen. Echter, een deel van de Nederlandse bedrijven blijft nog achter in het nemen van voldoende cybermaatregelen[12].

Het Cybersecuritybeeld Nederland (CSBN) 2022 laat zien dat er een groot verschil bestaat in cybervolwassenheid tussen organisaties[13]. Er is sprake van een groeiende cyberweerbaarheidskloof tussen bedrijven die succesvol cyberrisico's en afhankelijkheden kunnen inschatten en de weerbaarheid van hun organisatie hierop kunnen aanpassen, en bedrijven die hier nog onvoldoende in slagen. In het onderzoek richten wij ons op het midden- en kleinbedrijf (mkb) omdat daar de meeste achterblijvers lijken te zijn (zie 2.3.2). Gezien het grote maatschappelijke belang van het mkb, heeft een onvoldoende mate van cyberweerbaarheid niet alleen potentiële gevolgen voor de individuele bedrijven in het mkb, maar ook voor de bredere productieketens waarvan zij deel uitmaken, indien ketenpartners geraakt worden door cyberincidenten. Dit zet de algehele cyberweerbaarheid van onze samenleving onder druk en maakt ons land kwetsbaar voor digitale dreigingen.

Om inzicht te krijgen in de cyberweerbaarheidskloof heeft de minister van Justitie en Veiligheid de Cyber Security Raad (CSR) verzocht om een advies uit te brengen en antwoord te geven op de volgende vragen:

1. Wat zijn de **oorzaken van de cyberweerbaarheidskloof** en de mogelijkheden om te komen tot een **objectieve metriek/ indicatoren** voor cyberweerbaarheid van Nederlandse organisaties?
2. **Welk soort hulp is er nodig** om organisaties bewust te maken van de noodzaak om risicoanalyses te laten maken, afhankelijkheden in hun eigen keten van toeleveranciers in kaart te laten brengen, en **zelf voldoende cyberveiligheidsmaatregelen te laten treffen,** gegeven hun risicoprofiel en (beoogd) volwassenheidsniveau?
3. Welke (overheids-)interventies en adviezen zijn het meest effectief om vervolgens de kloof te verkleinen? Welke tools werken het beste in welke omgeving? **Hoe partijen aan te zetten tot handelen?**
4. In hoeverre kunnen we als Nederland hierbij **leren van andere landen.** Wat werkt wel/niet, bijvoorbeeld in het Verenigd Koninkrijk, Duitsland en Frankrijk waar al bepaalde initiatieven voor het mkb zijn ontplooid?

Dit onderzoek, uitgevoerd door Deloitte in opdracht van de Cyber Security Raad, draagt bij aan de beantwoording van de gestelde vragen door onder andere: (1) oorzaken van de cyberweerbaarheidskloof te identificeren, (2) de beschikbare hulpmiddelen vanuit de overheid en niet-commerciële hulpmiddelen vanuit het bedrijfsleven in kaart te brengen, en (3) mogelijkheden om de kloof te verkleinen te onderzoeken, inclusief potentiële nieuwe beleidsinitiatieven gebaseerd op ervaringen vanuit het buitenland. Het direct in contact treden met mkb-bedrijven, om inzicht te krijgen in hun realiteit, mogelijkheden en behoeftes, is een essentieel en onderscheidend onderdeel van het onderzoek. Dit alles met het doel de Cyber Security Raad in staat te stellen de vragen van de minister op een onderbouwde manier te kunnen beantwoorden.

[9] Nederlandse Cybersecuritystrategie 2022–2028, Nationaal Coördinator Terrorisme-bestrijding en Veiligheid (2022)
[10] Cyberbeveiliging: EU-aanpak van cyber¬dreigingen, Europese Raad (2023)
[11] Cybersecurity Woordenboek, CyberVeilig Nederland
[12] Rapport Digitale weerbaarheid zzp en mkb, Digital Trust Center (DTC) Benchmark onderzoek (2023)
[13] Cybersecuritybeeld Nederland 2022, Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022)

1.2 Aanpak van het onderzoek

Dit rapport geeft antwoord op de onderstaande onderzoeksvragen, geformuleerd door de Cyber Security Raad. De onderzoeksvragen zijn onderdeel van een uitgebreide uitvraag, en zijn een doorvertaling van de compacte vragen van de minister.

Hoofdvraag 1: Waarom is er een cyberweerbaarheidskloof en welke mogelijkheden zijn er voor bedrijven om hun cyberweerbaarheidsniveau in kaart te brengen?

- **Subvraag 1:** Wat zijn mogelijke verklaringen voor een suboptimaal cyberweerbaarheidsniveau bij bedrijven (in termen van onderinvestering)?
- **Subvraag 2:** Welke (publiek-private) mogelijkheden/ tools bestaan er om bedrijven in staat te stellen hun huidige eigen cyberweerbaarheidsniveau en hun optimaal cyberweerbaarheidsniveau te identificeren (bijvoorbeeld: metrieken, interventies, instrumentarium, classificaties van bedrijven en sectoren, etc.), en hoe goed werken die tools?

Hoofdvraag 2: Welke mogelijkheden zijn er voor de overheid om bedrijven te helpen om hun cyberweerbaarheidsniveau naar een voor hen optimaal niveau te brengen, met als resultaat dat bedrijven daadwerkelijk gebruik maken van deze mogelijkheden?

- **Subvraag 3:** Welke beleidsmaatregelen werken wel en niet om bedrijven te stimuleren hun huidige en optimale cyberweerbaarheidsniveau in kaart te brengen?
- **Subvraag 4:** Hoe kunnen we stimuleren dat bedrijven weten hoe ze hun cyberweerbaarheid moeten versterken en dat ze vervolgens deze verbeteringen ook willen en kunnen doorvoeren?[14]

Voor dit onderzoek is deskresearch en literatuuronderzoek uitgevoerd om tot de initiële bevindingen te komen. Deze bevindingen zijn vervolgens gevalideerd en aangevuld door middel van:

- Een klankbordgroep bestaande uit 10 afgevaardigden vanuit bedrijven binnen het mkb, samenwerkingsverbanden, brancheorganisaties en de overheid[15];
- 32 interviews met bedrijven binnen het mkb[16];
- Aanvullende interviews met experts op het gebied van cyberweerbaarheid vanuit branche- en koepelorganisaties, samenwerkingsverbanden en ICT-leveranciers.

Er zijn twee bijeenkomsten georganiseerd met de klankbordgroep om resultaten te valideren en nieuwe inzichten op te halen. Er zijn twee overleggen georganiseerd met de CSR Subcommissie 'Cyberweerbaarheidskloof' om de voortgang van het project te bespreken.

Het onderzoek bestaat uit twee fasen. Tijdens de eerste fase ligt de nadruk op een verkenning waarbij op basis van deskresearch en literatuuronderzoek de oorzaken van de kloof en de hulpmiddelen[17] in kaart worden gebracht. Vervolgens worden deze uitkomsten getoetst met de klankbordgroep. Hiermee wordt antwoord gegeven op hoofdvraag 1, met uitzondering van het deel waarin wordt nagegaan hoe goed de tools werken. Dit wordt onderzocht in de tweede fase waarin de nadruk ligt op verdieping, waarbij onderzoek wordt gedaan naar de werking van de hulpmiddelen onder andere door middel van gesprekken met mkb-bedrijven. Ook ligt nadruk op de mogelijkheden die daadwerkelijk bijdragen aan het verkleinen van de kloof. Hiermee wordt antwoord gegeven op hoofdvraag 2. De twee fases zijn inhoudelijk nauw aan elkaar verbonden, de resultaten van de verkennende fase vormen de basis voor de verdiepende fase. De resultaten van beide fases zijn bijeengebracht in dit rapport.

1.3 Scope van het onderzoek

De scope van het onderzoek is gericht op:

1. Het Nederlandse mkb

De focus van dit onderzoek ligt op het mkb. In dit onderzoek wordt de definitie van het Centraal Bureau voor de Statistiek (CBS) gehanteerd: Alle bedrijven met 1 tot en met 249 werknemers. Deze definitie wordt ook gebruikt door het Digital Trust Center (DTC) dat ondernemers helpt met veilig digitaal ondernemen. Het CBS maakt onderscheid tussen verschillende categorieën binnen het mkb:

- 1-9 werknemers - microbedrijf,
- 10-49 werknemers - kleinbedrijf,
- 50-249 werknemers - middelgroot bedrijf[18].

Volgens de Kamer van Koophandel waren er op 1 januari 2023 1.269.579 zzp'ers, 355.118 parttime zzp'ers en 450.034 mkb'ers; een totaal van 2.074.731, dit zijn dus alle bedrijven in Nederland met 249 werknemers of minder[19]. Overheidsorganisaties, medeoverheden en burgers maken geen onderdeel uit van dit onderzoek.

2. Sectorale inzichten

Om inzicht te krijgen in (mogelijke) sectorale verschillen worden de bedrijven onderverdeeld in sectoren. Dit wordt gedaan aan de hand van de SBI-code. Elk bedrijf staat bij de Kamer van Koophandel ingeschreven met een SBI (Standaard Bedrijfsindeling) code. Deze SBI-codes zijn door de onderzoekers onderverdeeld in een lijst van sectoren. Deze lijst wordt in dit onderzoek als uitgangspunt voor de sectorale indeling gehanteerd. Het overzicht van sectoren is opgenomen in Appendix B – Overzicht Sectoren.

[14] Bij de beantwoording van deze subvraag wordt met 'we' gerefereerd naar de overheid
[15] De samenstelling van de klankbordgroep staat vermeld in Appendix A – Leden van de klankbordgroep
[16] De namen van de 32 geïnterviewde bedrijven zijn geanonimiseerd
[17] Zie Appendix C – Begrippenlijst voor de definitie van het begrip 'hulpmiddelen'
[18] Het Nederlandse midden- en kleinbedrijf Europees vergeleken, Centraal Bureau voor de Statistiek (2021)
[19] Zie KVK.nl, 'Data over de bedrijvendynamiek – 2023 1e kwartaal'

3. Aanpak in een aantal vergelijkbare landen
Ook andere landen hebben met dit vraagstuk te maken. Om nieuwe inzichten te verkrijgen met betrekking tot de aanpak om achterblijvende bedrijven binnen het mkb te ondersteunen bij het versterken van hun cyberweerbaarheid, is er input opgehaald uit de volgende vergelijkbare landen: Het Verenigd Koninkrijk, Duitsland, Denemarken en Frankrijk. De vergelijkbaarheid tussen de landen betreft aspecten op het gebied van economische ontwikkeling, de omvang van de digitale infrastructuur, het niveau van technologische ontwikkeling en de regelgeving omtrent cyberveiligheid.

1.4 Structuur van het rapport

In dit rapport worden de onderzoeksvragen beantwoord aan de hand van de volgende structuur:

Hoofdstuk 1. Introductie
In hoofdstuk 1. Introductie wordt de achtergrond van het onderzoek beschreven, inclusief de vragen van de minister van Justitie en Veiligheid waar de Cyber Security Raad gevraagd is een advies op uit te brengen. Verder bevat de introductie een korte toelichting van de aanpak en onderzoeksvragen, de scope en de structuur van het rapport.

Hoofdstuk 2. Definitie en huidige staat
In hoofdstuk 2. Definitie en huidige staat wordt dieper ingegaan op het concept cyberweerbaarheid, de cyberweerbaarheidskloof en de relatie met het mkb. Er wordt toegelicht wat wordt verstaan onder een optimaal cyberweerbaarheidsniveau, wat de huidige status is van de cyberweerbaarheid binnen het mkb en wat de Nederlandse (overheids-)aanpak voor cyberweerbaarheid op dit moment is.

Hoofdstuk 3. Obstakels die leiden tot de kloof
Hoofdstuk 3. Obstakels die leiden tot de kloof geeft inzicht in de obstakels die het mkb zelf ervaart in het behalen van een optimaal cyberweerbaarheidsniveau. Hierbij wordt onderscheid gemaakt tussen interne en externe obstakels; respectievelijk zijn dit de obstakels waar bedrijven zelf invloed op kunnen uitoefenen, en obstakels waar ze niet direct invloed op kunnen uitoefenen.

Hoofdstuk 4. Overzicht huidige hulpmiddelen
In hoofdstuk 4. Overzicht huidige hulpmiddelen wordt een inventarisatie gemaakt van publiek en private hulpmiddelen die bedrijven binnen het mkb kunnen gebruiken om hun cyberweerbaarheid te versterken. Hierin wordt onderscheid gemaakt tussen algemeen beschikbare hulpmiddelen, en hulpmiddelen vanuit private samenwerkingsverbanden. De hulpmiddelen zijn gekoppeld aan de eerder geïdentificeerde obstakels om inzicht verstrekken in het primaire doel van elk hulpmiddel.

Hoofdstuk 5. Stimuleren en verbeteren
Hoofdstuk 5. Stimuleren en verbeteren beantwoord de vraag hoe bedrijven binnen het mkb gestimuleerd kunnen worden om hun cyberweerbaarheid te verbeteren. Hierbij wordt aan de hand van de obstakels gekeken of de aangeboden hulp aansluit bij de behoefte van bedrijven binnen het mkb. Op basis van interviews en voorbeelden uit vergelijkbare landen wordt vervolgens gekeken naar mogelijke oplossingen voor elk obstakel.

Verder wordt er gekeken naar de vindbaarheid, het gebruik en de effectiviteit (door middel van periodieke evaluaties) van de aangeboden hulp vanuit het perspectief van de aanbieders van de hulp. Het betreft hier geen evaluatie op het niveau van de individuele hulpmiddelen maar een meta-analyse van de aangeboden hulp.

Hoofdstuk 6. Mogelijkheden om te komen tot een metriek
Hoofdstuk 6. Mogelijkheden om te komen tot een metriek presenteert mogelijkheden om te komen tot een objectieve metriek voor het in kaart brengen van het huidige en optimale cyberweerbaarheidsniveau van een bedrijf, inclusief maatregelen die nodig zijn voor het verhogen van het huidige niveau tot het optimale niveau. Dit wordt gedaan aan de hand van een inventarisatie van de bestaande metrieken en een evaluatie van deze metrieken aan de hand van voorwaarden voor het mkb.

Hoofdstuk 7. Conclusies en aanbevelingen
Hoofdstuk 7. Conclusies en aanbevelingen is een synthese van het gehele onderzoek, waarbij de belangrijkste conclusies en aanbevelingen gepresenteerd worden door antwoord te gegeven op de onderzoeksvragen zoals opgesteld door de Cyber Security Raad.

2. Definitie en huidige staat

2. Definitie en huidige staat

2.1 Definitie cyberweerbaarheid

Cyberweerbaarheid omvat het vermogen van een bedrijf om (relevante) digitale risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen, en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken[20]. Dit heeft betrekking op de veerkracht van een bedrijf om zich te verdedigen tegen, aan te passen aan, te herstellen en te leren van cyberaanvallen en andere digitale dreigingen.

De cyberweerbaarheidskloof kan beschreven worden aan de hand van het huidige cyberweerbaarheidsniveau versus het optimale cyberweerbaarheidsniveau van een bedrijf. De huidige cyberweerbaarheid van een bedrijf is het vertrekpunt, en de optimale cyberweerbaarheid is het beoogde doel dat nodig is om vastgestelde risico's afdoende te mitigeren om digitaal weerbaar te zijn. Bedrijven waarbij het huidige niveau van cyberweerbaarheid ook het optimale niveau van cyberweerbaarheid betreft (of daar heel dichtbij zit) hebben hun cybersecurityrisico's onder controle, terwijl er ook bedrijven zijn waarbij het huidige cyberweerbaarheidsniveau ver achterblijft bij het optimale niveau. Het huidige en optimale niveau worden hieronder verder toegelicht en zijn van belang in het definiëren van de cyberweerbaarheidskloof.

2.2 Huidige en optimale cyberweerbaarheid

2.2.1 Huidige cyberweerbaarheid

Om zicht te krijgen op het huidige cyberweerbaarheidsniveau van een bedrijf dient deze objectief gemeten te worden; hier zijn op dit moment verschillende manieren voor:

1. **Cybermaatregelen in kaart brengen voor individuele bedrijven.** Het DTC biedt de 'CyberVeilig Check'[21] aan voor zzp'ers en mkb'ers. Dit is een online vragenlijst waarmee vastgesteld wordt welke beveiligingsmaatregelen binnen het bedrijf geïmplementeerd zijn; denk bijvoorbeeld aan antivirus, tweestapsverificatie, het automatisch updaten van mobiele apparaten, etc.
2. **Cybermaatregelen in kaart brengen voor een groep bedrijven.** Het CBS meet middels de Cybersecuritymonitor voor een groep bedrijven welke cybermaatregelen zij hebben geïmplementeerd[22]. Een ander voorbeeld is een onderzoek van het DTC naar de ICT-kenmerken van bedrijven die aangesloten zijn bij netwerkorganisaties waar het DTC mee samenwerkt (DTC-bedrijven). Uit dit onderzoek blijkt dat DTC-bedrijven gemiddeld genomen meer veiligheidsmaatregelen nemen dan een referentiegroep bedrijven met eenzelfde samenstelling die niet samenwerken met het DTC.[23]
3. **Cybermaatregelen in kaart brengen en koppelen aan een cyberweerbaarheidsscore.** Er zijn securitybedrijven die aan de hand van indicatoren een cyberweerbaarheidsscore vaststellen van hun klanten. Deze indicatoren gaan verder dan alleen technische beveiligingsmaatregelen, en omvatten ook maatregelen rondom cyberbeleid en -bewustzijn binnen een bedrijf om zo een totaalbeeld te krijgen van de cyberweerbaarheid.

Bij het vaststellen van de huidige cyberweerbaarheid van een bedrijf is het belangrijk om ook maatregelen mee te nemen die nodig zijn om te herstellen en te leren van cyberaanvallen en digitale dreigingen. Het leer- en herstelvermogen wordt ook meegenomen in hoofdstukken 4 en 5 van dit onderzoek.

2.2.2 Optimale cyberweerbaarheid

De optimale cyberweerbaarheid is het beoogde doel van een bedrijf. Dit optimale niveau is nodig om de relevante digitale risico's voor het bedrijf voldoende af te dekken. Het totaalpakket aan risico's (het risicoprofiel) wordt onder andere bepaald door de aard van een bedrijf, de sector en de keten waarin het actief is, de digitale infrastructuur en de gevoeligheid van data en het dreigingslandschap[24]. Het optimale cyberweerbaarheidsniveau is dus afhankelijk van het risicoprofiel, en verschilt daarom ook per bedrijf[25].

Als gevolg van het snel veranderende dreigingslandschap is het noodzakelijk dat bedrijven structureel hun optimale cyberweerbaarheidsniveau bepalen en vervolgens de juiste cybersecuritymaatregelen treffen[26]. Bedrijven moeten naar het bij hen passende optimale cyberweerbaarheidsniveau streven om de voor hen relevante digitale risico's te beheersen en de bedrijfsvoering en/of dienstverlening te beschermen. Hierbij dient rekening gehouden te worden met de gehele productieketen waar de bedrijven onderdeel van uitmaken; zowel leveranciers als klanten kunnen eisen stellen met betrekking tot de cybersecuritymaatregelen die genomen moeten worden. Ook dient er rekening gehouden te worden met de kosten. Een optimaal cyberweerbaarheidsniveau moet praktisch en realistisch zijn voor een bedrijf, rekening houdend met de vereiste investeringen om dit niveau te bereiken. Een te hoge drempel kan leiden tot financiële lasten, terwijl een te lage drempel de veiligheid van de bedrijven in gevaar kan brengen. Een juiste balans tussen de kosten en baten is dus essentieel om een optimaal cyberweerbaarheidsniveau te bereiken[27]. Deze balans is bereikt wanneer de kosten van investeringen in cyberweerbaarheid gelijk staan aan de baten in termen van gereduceerd risico[28]. De mate waarin risico's gereduceerd dienen te worden hangt af van de risicobereidheid van een organisatie waarin de keuze wordt gemaakt bepaalde risico's wel of niet te accepteren.

[20] Cybersecurity Woordenboek, Cyberveilig Nederland
[21] Zie tools.digitaltrustcenter.nl/cyberveilig-check/
[22] Zie cbs.nl, Cybersecuritymonitor 2022
[23] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
[24] Stappenplan risicoanalyse, Digital Trust Center
[25] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[26] Cybersecuritybeeld Nederland 2023, Nationaal Coördinator Terrorismebestrijding en Veiligheid, (2022)
[27] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[28] The Law and Economics of Cyber Security, B.F.H. Nieuwesteeg (2018)

Net als het huidige cyberweerbaarheidsniveau is het belangrijk dat bedrijven hun optimale cyberweerbaarheidsniveau in kaart brengen. Een meetinstrument waarmee een objectieve, kwantitatieve score bepaald kan worden voor de cyberweerbaarheid van een bedrijf wordt in dit rapport gedefinieerd als een metriek. Dit zal verder worden toegelicht in hoofdstuk 6.

2.3 Definitie cyberweerbaarheidskloof

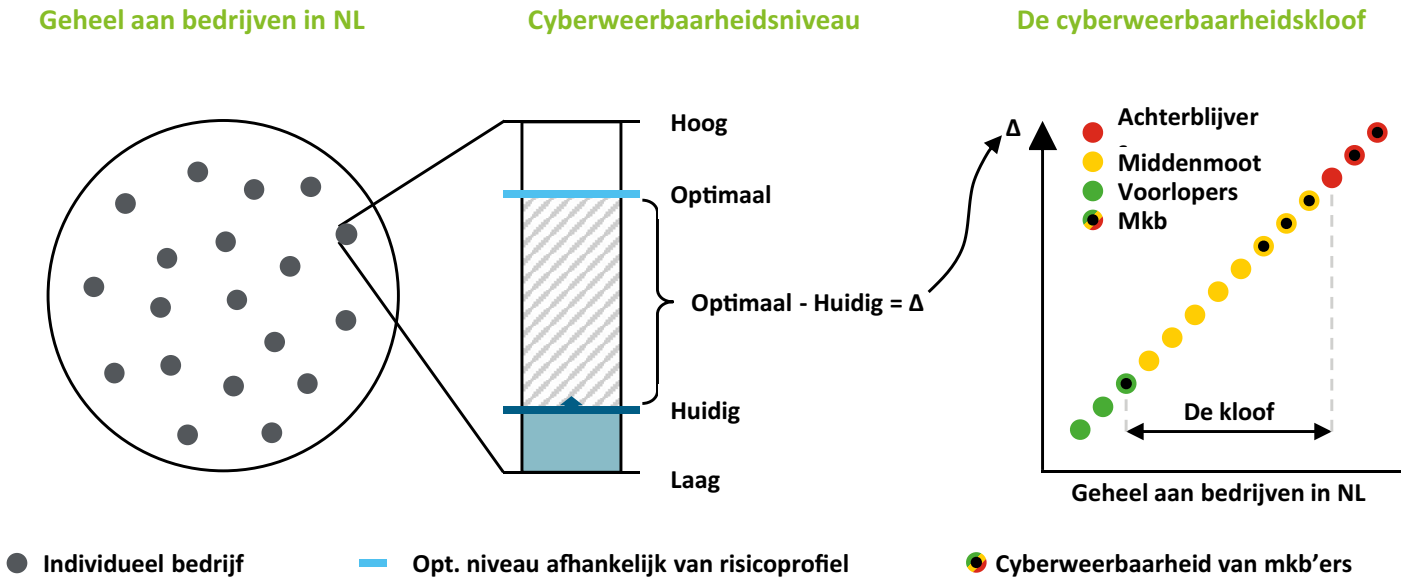
2.3.1 Definitie cyberweerbaarheidskloof

Er is een groeiende kloof vastgesteld tussen bedrijven in Nederland die goed in staat zijn hun cyberrisico's en afhankelijkheden in te schatten en hun weerbaarheid daarop aan te passen (naar een optimaal niveau), versus bedrijven die daar minder goed in slagen[29]; in andere woorden: er is een kloof tussen voorlopers en achterblijvers. Deze termen worden als volgt gedefinieerd:

- **Voorlopers:** bedrijven met een huidig cyberweerbaarheidsniveau dat dicht rond hun optimale niveau ligt. Dit betekent dat het bedrijf weet wat het risicoprofiel is en het optimale cyberweerbaarheidsniveau, en erin slaagt het huidige cyberweerbaarheidsniveau te verhogen naar een (zo goed als) optimaal niveau, en dit ook weet te behouden.
- **Achterblijvers:** bedrijven met een huidig cyberweerbaarheidsniveau dat ver onder hun optimale niveau ligt. Dit betekent dat het bedrijf of 1) haar huidige en/of optimale cyberweerbaarheidsniveau niet kent, of 2) deze niveaus wel kent maar er bewust niet voor kiest of onvoldoende in slaagt de cyberweerbaarheid te versterken.

Figuur 2 (onderstaand) visualiseert het concept van de cyberweerbaarheidskloof. Elk bedrijf in Nederland, zowel binnen en buiten het mkb, heeft dus een huidig en optimaal cyberweerbaarheidsniveau.

Zoals gezegd is het optimale cyberweerbaarheidsniveau afhankelijk van het type bedrijf. Een bakker hoeft in absolute termen niet even cyberweerbaar te zijn als een internationaal tech-bedrijf in de medische sector. Als bedrijven onderling worden vergeleken, is dus het verschil tussen het optimale en huidige niveau van belang. Dit verschil definieert dus of een bedrijf voorloopt of achterblijft in vergelijking met andere bedrijven. Een bedrijf dat vooroploopt hoeft dus niet per se de meeste beveiligingsmaatregelen geïmplementeerd te hebben.



Figuur 2 De cyberweerbaarheidskloof. Een achterblijver wordt gedefinieerd als een bedrijf met een huidige cyberweerbaarheid dat ver onder het optimale niveau ligt.

[29] Benchmark Onderzoek, Digital trust Center (2023)

2.3.2 Het in kaart brengen van de cyberweerbaarheidskloof

Het is mogelijk voor een individueel bedrijf hun huidige en optimale cyberweerbaarheid in kaart te brengen. Maar om vervolgens bedrijven onderling te vergelijken en zo de cyberweerbaarheidskloof in kaart te brengen is niet eenvoudig. Er is namelijk geen gestandaardiseerde metriek en risicoanalyse beschikbaar waarmee alle bedrijven in Nederland op een uniforme manier hun huidige en optimale cyberweerbaarheidsniveaus kunnen meten en vergelijken (zie ook Hoofdstuk 6. Mogelijkheden om te komen tot een metriek). Hierdoor is het dus ook lastig om op een grote schaal de achterblijvers te identificeren.

Een eerste stap om op grote schaal toch achterblijvers te identificeren zou kunnen door bedrijven te identificeren die relatief weinig cyberweerbaarheidsmaatregelen hebben geïmplementeerd. De aanname hier is dan dat de kans groter is dat een bedrijf een suboptimaal cyberweerbaarheidsniveau heeft als het relatief minder cyberweerbaarheidsmaatregelen heeft geïmplementeerd.

Ook binnen het mkb zijn er bedrijven die voorlopen en bedrijven die achterblijven. Echter is het ook binnen het mkb lastig om achterblijvers te identificeren. Het richten op het totale mkb voor het verkleinen van de algehele cyberweerbaarheidskloof in Nederland lijkt daarom een effectieve aanpak. De Cybersecuritymonitor van 2022[30] laat zien dat het percentage van bedrijven dat bepaalde ICT-veiligheidsmaatregelen heeft geïmplementeerd afneemt met het aantal werknemers. Ook laat de data zien dat bedrijven met minder werknemers, minder vaak een risicoanalyse uitvoeren. Zo ontstaat het beeld dat bedrijven binnen het mkb (dit is inclusief zzp'ers) ten opzichte van het geheel, gemiddeld genomen minder cyberweerbaar zijn en minder zicht hebben op hun optimale cyberweerbaarheidsniveau.

Binnen dit onderzoek komt dit beeld ook naar voren in de 32 gesprekken die zijn gevoerd met mkb'ers; dit blijkt uit:

- 44% van de geïnterviewden geeft aan een penetratietest/ risicoanalyse uit te hebben gevoerd (zie Figuur 11 in Appendix F – Interviewdata). Volgens het CBS is het percentage van bedrijven met 250 of meer werknemers dat een risicoanalyse heeft uitgevoerd zelfs ruim 80%.
- 50% van de geïnterviewden geeft aan dat 'onvoldoende inzicht in risico's' een obstakel is in het versterken van hun cyberweerbaarheid (zie Figuur 10 in Appendix F – Interviewdata).
- 47% van de geïnterviewden spreekt de behoefte uit aan 'handelingsperspectief' dat aansluit op het risicoprofiel (zie Figuur 12 in Appendix F – Interviewdata), ofwel, concrete maatregelen die genomen kunnen worden op basis van de risico's die het bedrijf loopt.

2.4 Onderscheidende variabelen binnen het mkb

Het mkb omvat een diverse groep aan bedrijven. Om rekening te houden met deze diversiteit is een viertal onderscheidende variabelen geïdentificeerd[31]. Dit is van belang omdat de variabelen samenhangen met de obstakels die bedrijven ervaren bij het versterken van hun cyberweerbaarheid, het risicoprofiel van het bedrijf, investeringsmogelijkheden en uiteindelijk hun cyberweerbaarheidsniveau. In gesprekken met brancheorganisaties en beleidsmakers kwam duidelijk naar voren dat er behoefte bestaat aan gedifferentieerde inzichten. Echter is er binnen dit onderzoek niet verder gedifferentieerd dan de onderstaande variabelen vanwege de gekozen onderzoeksmethode.

1. Aantal werknemers

Het mkb is het geheel aan private bedrijven in Nederland met een medewerkers aantal tussen de 1 en 249[32]. In dit onderzoek worden de volgende vier categorieën gehanteerd:

1. **ZZP:** 1 werknemer
2. **Micro bedrijf:** 2-9 werknemers
3. **Klein bedrijf:** 10-49 werknemers
4. **Middelgroot bedrijf:** 50-249 werknemers

De CBS Cybersecurity Monitor biedt inzichten in de relatie tussen de grootte van bedrijven, de genomen cybermaatregelen en de digitale ontwikkelingen in de periode van 2016 tot 2021. Middelgrote bedrijven nemen bijvoorbeeld doorgaans meer cybermaatregelen dan kleinere bedrijven[33].

2. Gebruik van standaard of op maat gemaakte ICT-oplossingen en informatiebeveiligingsdiensten

Bedrijven binnen het mkb kunnen gebruikmaken van standaard of op maat gemaakte ICT-oplossingen en informatiebeveiligingsdiensten.

1 **Standaard ICT-oplossingen en informatiebeveiligings-diensten** zijn diensten of producten die worden aangeboden door externe technologiebedrijven voor een breed scala aan gebruikers en sectoren; denk bijvoorbeeld aan Microsoft Office, Adobe, Typeform, Exact Online, Meta Business Suite, Google Drive, Moneybird, Zoom, etc. Deze ICT-oplossingen en informatiebeveiligingsdiensten bieden vaak ook cybermaatregelen aan waar bedrijven binnen het mkb gebruik van kunnen maken. Bedrijven die standaard ICT-oplossingen en informatiebeveiligingsdiensten (inclusief cloudoplossingen) gebruiken kunnen profiteren van regelmatige updates en patches die door de leverancier worden verstrekt.

[30] Cyber Security Monitor 2022, Centraal Bureau voor de Statistiek (2023)
[31] De variabelen zijn in afstemming met de klankbordgroep geïdentificeerd
[32] Het Nederlandse midden- en kleinbedrijf Europees vergeleken, Centraal Bureau voor de Statistiek (2021)
[33] Cyber Security Monitor 2022, Centraal Bureau voor de Statistiek (2023)

2. **Op maat gemaakte ICT-oplossingen en informatie-beveiligingsdiensten** zijn ontwikkeld om te voldoen aan de specifieke behoeftes van een bedrijf en omvatten, in tegenstelling tot de standaard ICT-oplossingen en informatiebeveiligingsdiensten, specifieke functionaliteiten. Bij deze ICT-oplossingen en informatiebeveiligings-diensten is het vaak aan de bedrijven binnen het mkb zelf om de cybermaatregelen te implementeren of om dit door een externe partij te laten doen (bijvoorbeeld door middel van een 'Managed Security Service Provider' (MSSP)). Bedrijven kunnen met op maat gemaakte software mogelijk meer controle uitoefenen op de implementatie van cybermaatregelen die specifiek zijn ontworpen op basis van de behoeftes van het bedrijf. Echter, bij op maat gemaakte oplossingen (specifiek voor de organisatie) kan een organisatie niet profiteren van de schaalvoordelen en bijbehorende cyberveiligheidscapaciteit van standaard ICT-oplossingen.
3. **NIS2-richtlijn**
   Vanuit de Europese Unie is een pakket aan maatregelen afgekondigd dat gericht is op het versterken van de cyberveiligheid en cyberweerbaarheid van organisaties en het beschermen van burgers en consumenten. Een van deze richtlijnen is de Network and Information Security directive (NIS2). De NIS2-richtlijn vereist dat bedrijven in de Europese Unie die als 'essentieel' of 'belangrijk' worden aangemerkt, voldoen aan strengere cybermaatregelen om digitale dreigingen te voorkomen. Nederland zal de NIS2-richtlijn opnemen in de Wet Beveiliging Netwerk en Informatiesystemen (Wbni) en/of de wet Digitale Veiligheid. Kenmerkend aan de richtlijn is de invoering van bestuursaansprakelijkheid en het feit dat de richtlijn gericht is op de gehele toeleveranciersketen. Het wel of niet moeten implementeren van de NIS2-normen door bedrijven zal effect hebben op de cyberweerbaarheid van bedrijven. Er wordt in dit onderzoek onderscheid gemaakt tussen:
   1. **Bedrijven die onder de NIS2-richtlijn vallen:** Bedrijven die onder de NIS2-richtlijn vallen worden gekenmerkt als 'essentiële' of 'belangrijke' entiteit en zullen volgens de richtlijn vanuit de Europese Unie per oktober 2024 moeten voldoen aan strengere wettelijke eisen omtrent cyberveiligheid. In Nederland zal dit enige vertraging oplopen en zal dit voor alsnog (begin) 2025 zijn[34]. Hierdoor zullen deze bedrijven mogelijk meer prioriteit geven aan cyberweerbaarheid.
   2. **Bedrijven die niet onder de NIS2-richtlijn vallen:** Bedrijven die niet onder de NIS2-richtlijn vallen, hebben geen verplichting in het naleven van de vereisten die de NIS2-richtlijn stelt.
   3. **Bedrijven die niet onder de NIS2-richtlijn vallen maar wel maatregelen zullen moeten nemen omdat ze in de toeleveringsketen vallen van een bedrijf dat wel onder de NIS2-richtlijn valt:** Bedrijven die niet onder de NIS2-richtlijn vallen, maar indirect worden geraakt door de richtlijn doordat zij in een toeleveranciersketen zitten van een bedrijf dat direct onder de NIS2-richtlijn valt, zullen ook moeten voldoen aan strengere eisen omtrent cyberveiligheid. Hierdoor zullen deze bedrijven mogelijk meer prioriteit geven aan cyberweerbaarheid, echter is het complex om deze toeleveranciersketen goed in kaart te brengen.

Of de geïnterviewde bedrijven wel of niet onder NIS2 vallen is niet meegenomen gezien de complexiteit van de benodigde informatie hiervoor (bijvoorbeeld: jaaromzet en balans laatst gesloten boekjaar, uitzonderingen die van toepassing zijn, bedrijf aangewezen als essentiële entiteit, etc.).

4. **Differentiatie branches en sectoren**
   De sector of branche waar een bedrijf binnen het mkb onder valt is van invloed op de cyberweerbaarheid van deze bedrijven[35]. Bedrijven die door de aard van hun werkzaamheden tot een bepaalde sector behoren krijgen mogelijk te maken met sectorspecifieke cyberdreigingen. Dit heeft invloed op welke cybermaatregelen zij dienen te implementeren[36]. Een voorbeeld hiervan is de financiële sector waar financiële instellingen onderdeel zijn van de kritieke infrastructuur en werken met gevoelige gegevens. Dit maakt deze instellingen een aantrekkelijk doelwit voor cybercriminelen. Hierdoor zijn er voor deze sector specifieke richtlijnen en voorschriften opgesteld die strengere minimumstandaarden op het gebied van cyberweerbaarheid oplegt aan financiële instellingen.

Binnen dit onderzoek is de diversiteit aan geïnterviewde bedrijven binnen het mkb in kaart gebracht in Tabel 1. De tabel toont 3 onderscheidende variabelen, met een onderverdeling van de in totaal 32 geïnterviewde bedrijven per variabele. De 3 variabelen zijn:

1. Aantal medewerkers
2. Standaard of op maat gemaakte ICT-oplossingen en informatiebeveiligingsdiensten
3. SBI-sector waarin het bedrijf actief is

[34] Zie brief regering 'Stand van zaken implementatie NIS2 en CER richtlijnen', Tweede Kamer der Staten-Generaal, 31 januari 2024
[35] Cyber Security Monitor 2022, Centraal Bureau voor de Statistiek (2023)
[36] Informatie verkregen vanuit de klankbordgroep tijdens de starbijeenkomst op 18-08-2023

Onderscheidende variabele	Aantal geïnterviewde mkb'ers (totaal 32)
Aantal medewerkers	
Middelgroot bedrijf (50-249)	12
Klein bedrijf (10-49)	14
Micro bedrijf (2-9)	4
ZZP (1)	2
Standaard of op maat gemaakte ICT-oplossingen en informatiebeveiligingsdiensten	
Standaard	24
Standaard en op maat gemaakt	8
SBI-sector waarin het bedrijf actief is	
C. Industrie	6
F. Bouwnijverheid	1
G. Groot- en detailhandel; reparatie van auto's	4
H. Vervoer en opslag	1
J. Informatie en communicatie	7
L. Verhuur van en handel in onroerend goed	2
M. Advisering, onderzoek en overige specialistische zakelijke dienstverlening	9
R. Cultuur, sport en recreatie	2

Tabel 1 Overzicht van het aantal geïnterviewde bedrijven binnen het mkb, per onderscheidende variabele.

2.5 De Nederlandse aanpak

In oktober 2022 is de 'Nederlandse Cybersecuritystrategie (NLCS) 2022-2028: Ambities en acties voor een digitaal veilige samenleving' gepubliceerd[37]. Met de NLCS streeft het kabinet naar een digitaal veilig Nederland. De Nederlandse aanpak voor het verbeteren van de cyberweerbaarheid omvat een stelsel van (sub-)doelen en acties waarbij de overheid, het bedrijfsleven en kennisinstellingen onder meer samenwerken om de cyberweerbaarheidskloof te verkleinen. Deze aanpak is deels gebaseerd op eerdere adviezen van de Cyber Security Raad[38] hierover. De overheid speelt een leidende rol bij het faciliteren van samenwerking, het bieden van expertise en het ontwikkelen van beleid. De afgelopen jaren zijn er initiatieven ontplooid en hulpmiddelen ontwikkeld om de cyberweerbaarheid van mkb'ers te verhogen.

Zo is in 2018 het DTC opgericht, met als missie om ruim twee miljoen Nederlandse bedrijven weerbaarder te maken tegen toenemende cyberdreigingen[39]. In 2022 is de Wbni aangepast zodat het NCSC de grondslag heeft om in ruimere zin dreigings- en incidentinformatie te delen met schakelorganisaties. Deze schakelorganisaties kunnen daarmee vervolgens organisaties in hun achterban van die informatie en advies voorzien. In bijzondere gevallen kan de dreigings- of incidentinformatie ook met andere aanbieders gedeeld worden[40].

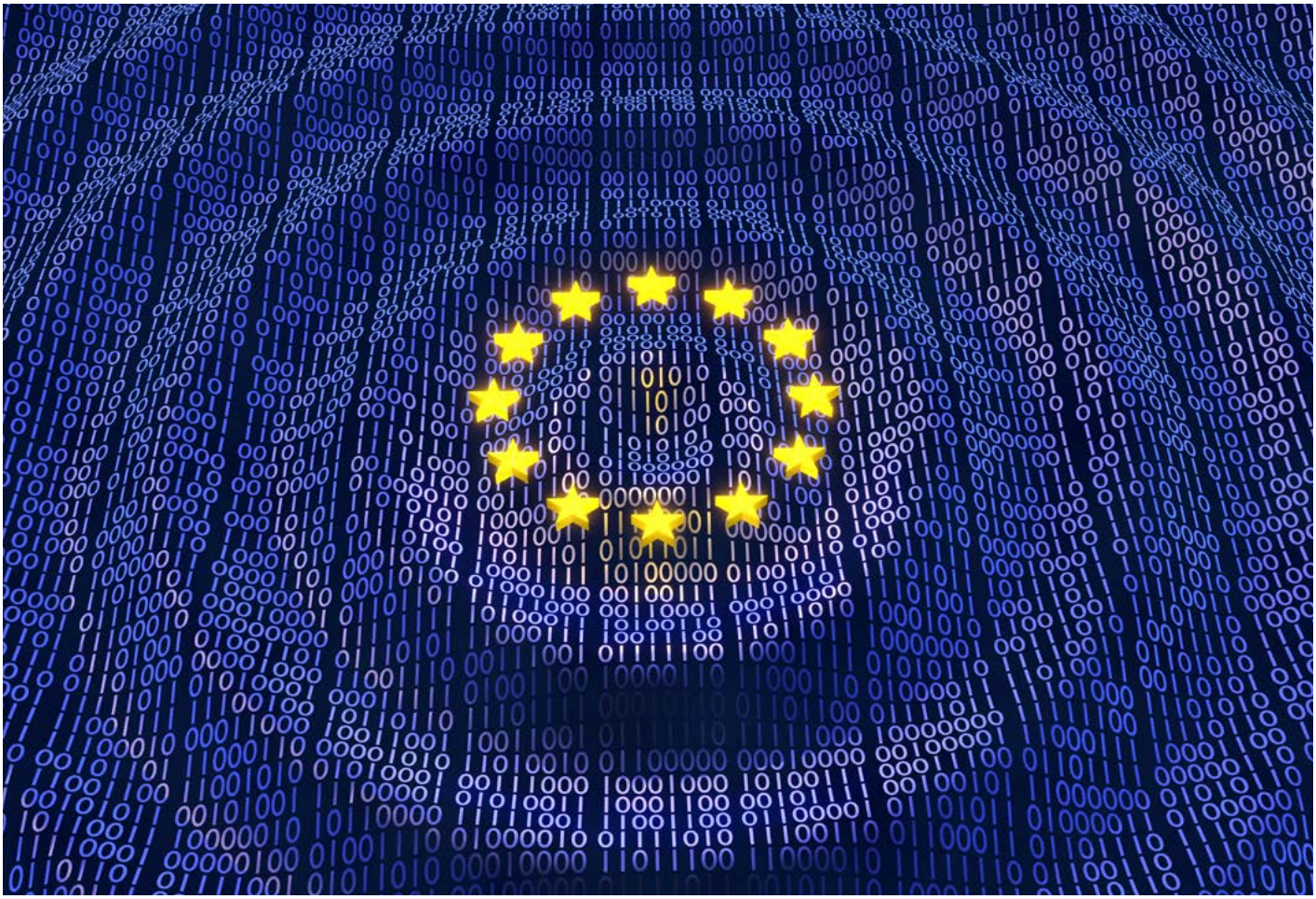
Het Landelijk Dekkend Stelsel (LDS) van informatieknooppunten moet er zorg voor dragen dat informatie met betrekking tot dreigingen, kwetsbaarheden en incidenten makkelijk toegankelijk is voor deze organisaties. Het DTC zal samengaan met het NCSC en het Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) in een centraal expertisecentrum en informatieknooppunt. Deze nieuwe instelling gaat alle organisaties in Nederland- groot en klein, publiek en privaat, vitaal en niet-vitaal- van passende kennis en informatie voorzien.

De overheid investeert structureel in de bestrijding van cybercriminaliteit. De Nationale Politie heeft een team 'High Tech Crime' dat focust op de meest geavanceerde vormen van cybercrime. Daarnaast zijn de afgelopen jaren gespecialiseerde cybercrimeteams op regionaal niveau versterkt. Internationaal werkt de politie nauw samen met onder meer Europol, Interpol en de FBI[41].

In de NLCS worden cybermaatregelen aangekondigd om bedrijven binnen het mkb te ontzorgen als het gaat om de proportionaliteit van cybermaatregelen en -eisen, en het leggen van de verantwoordelijkheden voor de veiligheid van digitale producten en diensten bij de overheid, producenten en dienstverleners, zonder de eigen verantwoordelijkheid voor de cyberweerbaarheid weg te nemen bij de bedrijven[42].

37 Nederlandse Cybersecuritystrategie 2022-2028, Rijksoverheid (2022)
38 Adviesrapport 'Integrale aanpak cyberweerbaarheid', Cyber Security Raad (2021)
39 Zie digitaltrustcenter.nl
40 Meer mogelijk NCSC om dreigings- en incidentinformatie te delen, Nationaal Cyber Security Centrum (2022)
41 Zie vraaghetdepolitie.nl, 'Wat doet de politie tegen cybercrime?'
42 Cyber Security Monitor 2022, Centraal Bureau voor de Statistiek (2023)

Naast de NIS2-richtlijn zal ook de Cyber Resilience Act (CRA) de cyberveiligheid van de samenleving te versterken. De wetgeving zal ervoor zorgen dat digitale producten aan strengere cybersecurityeisen moeten voldoen voordat ze in Europa op de markt komen. Dit heeft impact op bedrijven binnen het mkb die onder de wetgeving vallen, maar ook op de ICT-leveranciers die digitale producten leveren aan het mkb. Echter is maar een deel van de bedrijven binnen het mkb onderhevig aan de NIS2 of de CRA. Voor een groot deel is het Nederlandse mkb dus niet verplicht te voldoen aan deze nieuwe wetgeving. Verder zal het landelijke cybersecuritystelsel verstevigen door bijvoorbeeld het aanstellen van nationale CERTs (Computer Emergency Response Teams) en het delen van dreigings- en incidentinformatie, waar bedrijven binnen het mkb ook weer hun voordeel mee kunnen doen.



3. Obstakels die leiden tot de kloof

3. Obstakels die leiden tot de kloof

3.1 Introductie

Dit hoofdstuk beschrijft welke obstakels bedrijven binnen het mkb ervaren in het behalen van een optimaal cyberweerbaarheidsniveau.

Het doel is om een overzicht te creëren van de grootste obstakels, om zo inzicht te krijgen in de verschillende elementen van de cyberweerbaarheidskloof en de onderliggende oorzaken die bedrijven binnen het mkb ervan kunnen weerhouden om hun cyberweerbaarheid te versterken. Vervolgens kan er worden gekeken welke hulpmiddelen beschikbaar moeten worden gesteld om de geïdentificeerde obstakels zoveel mogelijk weg te nemen, en of de huidige hulpmiddelen voldoende effectief zijn (zie hoofdstukken 4 en 5).

De definitie van een obstakel is datgene wat een bedrijf binnen het mkb ervan weerhoudt om de cyberweerbaarheid te verhogen van een suboptimaal niveau naar een optimaal niveau.

3.2 Aanpak inventarisatie obstakels

De aanpak om te komen tot een inventarisatie en categorisatie van obstakels bestaat uit drie stappen:

1. Inventariseren van obstakels door deskresearch en literatuur-onderzoek;
2. Categoriseren van obstakels;
3. Valideren van obstakels met de klankbordgroep.

1. Inventariseren van obstakels door deskresearch en literatuuronderzoek

Door middel van deskresearch en literatuuronderzoek zijn verschillende obstakels geïdentificeerd. Voor deskresearch en literatuuronderzoek zijn de volgende type bronnen gebruikt:

1. **Wetenschappelijke bronnen.** Wetenschappelijke bronnen zijn (peer-reviewed) artikelen gepubliceerd door wetenschappers.
2. **Onderzoeksinstituten.** Rapporten van onderzoeksinstituten zijn gepubliceerde beschrijvingen van wetenschappelijk onderzoek. Een onderzoeksrapport dat gebruikt is, is de 'Cyber Security Monitor' van het Centraal Bureau voor de Statistiek.
3. **Rapporten van overheidsinstanties.** Rapporten van overheidsinstanties, zoals het NCSC of het DTC.
4. **Rapporten van branche- of koepelorganisaties.** Publicaties van branche- of koepelorganisaties geven inzicht in trends en statistieken binnen specifieke sectoren.
5. **Whitepapers.** Whitepapers zijn bronnen van informatie die betrekking hebben op een specifiek onderwerp, geschreven door bedrijven of non-profit organisaties.

2. Categoriseren van obstakels

Om een duidelijk en gestructureerd overzicht te creëren van de obstakels zijn de bevindingen geclusterd in categorieën. De obstakels zijn te verdelen in interne en externe obstakels:

- Interne obstakels. Dit zijn obstakels waar bedrijven zelf invloed op kunnen uitoefenen. Er kan zeker hulp geboden worden vanuit externe partijen om deze obstakels op te lossen, maar uiteindelijk is het bedrijf zelf verantwoordelijk voor het maken van keuzes en implementeren van maatregelen voor deze obstakels. Een voorbeeld is onvoldoende cyberbewustzijn bij het personeel van een bedrijf binnen het mkb waardoor de kans op cyberincidenten toeneemt.
- Externe obstakels. Dit zijn obstakels waar bedrijven niet direct invloed op kunnen uitoefenen. Een voorbeeld is het algemeen tekort aan personeel met expertise in cyberveiligheid en ICT waardoor het lastig is voor bedrijven binnen het mkb om het kennisniveau omtrent cyberveiligheid te verhogen. Dit obstakel overstijgt een individueel bedrijf binnen het mkb en vraagt om initiatieven vanuit bijvoorbeeld de overheid en onderwijsinstellingen.

De interne obstakels zijn in 3 categorieën te verdelen, en de externe obstakels in 5 categorieën (zie hoofdstuk 3. Obstakels die leiden tot de kloof).

3. Valideren van obstakels

De gecategoriseerde lijst met obstakels is gevalideerd met de klankbordgroep en subcommissie. De leden van de klankbordgroep en subcommissie hebben op basis van hun ervaringen uit de praktijk de inzichten verder aangescherpt. De gecategoriseerde lijst met obstakels is vervolgens aangepast aan de hand van de ontvangen feedback.

3.3 Overzicht obstakels

Tabel 2 toont het overzicht van de interne en externe obstakels

	Obstakel	Omschrijving
	Intern	
1	Onvoldoende cyberbewustzijn en -kennis	Een verlaagd niveau van cyberbewustzijn en –kennis bij bedrijven binnen het mkb leidt ertoe dat deze bedrijven de ernst en frequentie van cyberdreigingen onderschatten
2	Onvoldoende inzicht in risico's en handelingsperspectief	Het gebrek aan inzicht in de cyberrisico's van een bedrijf en de beschikbare mogelijkheden om te handelen op basis van deze risico's heeft impact op bedrijfsvoering mb.t. cyberveiligheid
3	Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden	Bedrijven binnen het mkb hebben moeite met het inschatten welke investeringshoogte passend is bij hun optimale cyberweerbaarheidsniveau; verder is het lastig te bepalen welke ICT diensten/producten goed genoeg zijn om de risico's van het bedrijf af te dekken
	Extern	
4	Algemeen tekort aan personeel in Nederland met expertise in ICT en cyberveiligheid	Er is in Nederland een algemeen tekort aan personeel met expertise in zowel ICT als cyberveiligheid wat de investering in cyberexpertise belemmert
5	Beperkte toepasbaarheid huidige cyberrichtlijnen voor het mkb	Huidige cyberrichtlijnen bevatten vaak te algemene kaders en zijn opgesteld voor grotere bedrijven waardoor deze voor bedrijven binnen het mkb lastig te begrijpen zijn zonder ondersteuning van cyberexperts
6	Afhankelijkheidsrisico's in toeleveringsketen	De afhankelijkheid van externe leveranciers kan voor bedrijven binnen het mkb risico's meebrengen wanneer cyberrisico's onvoldoende door deze externe partij worden beheerst
7	Beperkte vindbaarheid van (overheids-)hulpmiddelen	Bedrijven binnen het mkb weten (overheids-)initiatieven op het gebied van cyberveiligheid niet altijd te vinden en/of zijn deze bedrijven niet op de hoogte van het bestaan van dergelijke initiatieven
8	Veranderend dreigingslandschap	Het is lastig voor bedrijven binnen het mkb om hun digitale infrastructuur volledig af te stemmen op de steeds meer geavanceerde cyberdreigingen en het continu veranderend dreigingslandschap

Tabel 2 Overzicht van interne (groen) en externe (blauw) obstakels die leiden tot een suboptimaal cyberweerbaarheidsniveau.

Hieronder volgt per obstakel een omschrijving en duiding van de impact voor bedrijven binnen het mkb. De alinea's 'versterkende factoren' beschrijven onderlinge relaties tussen obstakels. De analyse met de klankbordgroep liet zien dat er een volgordelijkheid en randvoorwaardelijkheid is tussen de interne obstakels en externe obstakels[43]. Het is bijvoorbeeld lastig om te investeren in cybermaatregelen (obstakel 3) als er geen inzicht in risico's of handelingsperspectief is (obstakel 2). Het gebrek aan inzicht in risico's kan weer veroorzaakt worden doordat bedrijven binnen het mkb zich niet bewust zijn van het feit dat ze deze inzichtelijk moeten maken, of hier niet de juiste kennis voor hebben (obstakel 1).

De externe obstakels zijn niet op deze manier aan elkaar gecorreleerd. Wel kunnen de externe obstakels van invloed zijn op interne obstakels. Het algemeen tekort aan personeel met expertise in cyber en ICT (obstakel 4) kan bijvoorbeeld leiden tot onvoldoende cyberbewustzijn en -kennis (obstakel 1) binnen het bedrijf. Hierbij is obstakel 4 een versterkende factor van obstakel 1.

3.3.1 Interne obstakels

Onvoldoende cyberbewustzijn en -kennis

Onvoldoende cyberbewustzijn en -kennis is het eerste interne obstakel dat bedrijven binnen het mkb ervaren in het behalen van een optimaal niveau van cyberweerbaarheid. Cyberbewustzijn verwijst naar de mate waarin mensen risico's herkennen en zich ervan bewust zijn de veiligheid van informatie en systemen in gevaar te kunnen brengen[44]. Cyberkennis verwijst naar het begrip en de vaardigheden die nodig zijn om digitale systemen, technologie, en cyberrisico's effectief te beheren en beveiligen.

Impact op cyberweerbaarheid

Cyberbewustzijn en -kennis zijn beide van belang om de urgentie van cyberveiligheid te kunnen begrijpen en daadwerkelijk cyberweerbaar te zijn. Bij het ontbreken van cyberbewustzijn en -kennis moet niet alleen gekeken worden naar het management maar ook naar de medewerkers binnen een organisatie.

[43] Informatie verkregen vanuit de klankbordgroep tijdens de starbijeenkomst op 18-08-2023
[44] Cybersecurity Woordenboek, Digital Trust Center (2023)

Indien de medewerkers van een bedrijf binnen het mkb zich niet bewust zijn van de mogelijke cyberdreigingen, kan dit een groot risico vormen voor de cyberweerbaarheid van de organisatie (bijvoorbeeld door het klikken op phishing links).

Bedrijven binnen het mkb verwachten vanwege hun omvang en de aard van hun werkzaamheden vaak geen doelwit te zullen zijn van, of niet kwetsbaar te zijn voor cyberaanvallen en cyberdreigingen. Dit leidt ertoe dat bedrijven binnen het mkb de ernst en frequentie van cyberaanvallen onderschatten, evenals hun rol op dit gebied als ketenpartner. Hierdoor kunnen deze bedrijven niet adequaat handelen om cyberincidenten te voorkomen, te detecteren of te herstellen van deze cyberincidenten[45,46].

Uit onderzoek in het Verenigd Koninkrijk blijkt dat dreigings-informatie die beschikbaar wordt gesteld door 'Computer Emergency Response Teams (CERT)' vaak niet geschikt is voor gebruikers met weinig kennis van cyberveiligheid. Aannemende dat de onderliggende problematiek, doelgroepen en CERT-structuren vergelijkbaar zijn met die in Nederland, kan het zijn dat de dreigingsinformatie ook hier niet geschikt is voor gebruikers met weinig kennis van cyberveiligheid. Uit hetzelfde onderzoek blijkt dat voor sommige bedrijven binnen het mkb geldt dat het uitbesteden van ICT de stimulans voor het rapporteren van cyberincidenten vermindert. Hierdoor is het lastig voor bedrijven binnen het mkb met weinig cyberkennis om te begrijpen wat de grootste cyberrisico's zijn voor hen en wat voor stappen zij kunnen nemen na een cyberincident[47].

Daarnaast zijn bedrijven binnen het mkb beperkt betrokken bij (wetenschappelijke) onderzoeken[48]. Andersom vindt kennis uit wetenschappelijk onderzoek naar cyberweerbaarheid nog onvoldoende zijn weg naar de markt[49]. Dit maakt het lastig voor bedrijven binnen het mkb om door middel van kennisdeling hun cyberweerbaarheid te versterken.

Versterkende factoren

Een factor die onvoldoende cyberbewustzijn en -kennis kan versterken, is het onvoldoende aantrekken of opleiden van gekwalificeerd personeel met expertise in ICT en cyberveiligheid. Tijdens de startbijeenkomst met de klankbordgroep werd opgemerkt dat het bezitten van algemene kennis op het gebied van ICT niet altijd toereikend is als het aankomt op het effectief implementeren van cybermaatregelen. Echter, er is een algemeen tekort aan personeel met expertise in cyber en ICT in Nederland en dat hindert bedrijven binnen het mkb in het aantrekken of opleiden van gekwalificeerd personeel. Dit is ook een van de externe obstakels die later in dit hoofdstuk beschreven worden.

Onvoldoende inzicht in risico's en het ontbreken van een handelingsperspectief

Onvoldoende inzicht in risico's en het ontbreken van een handelingsperspectief is het tweede interne obstakel dat bedrijven binnen het mkb ervaren in het behalen van een optimaal niveau van cyberweerbaarheid. Inzicht in risico's verwijst naar het vermogen van bedrijven om de aard en omvang van potentiële cyberrisico's te identificeren en te begrijpen. Inzicht in handelingsperspectief heeft betrekking op het begrip van welke cybermaatregelen er nodig zijn om de geïdentificeerde risico's te mitigeren.

Impact op cyberweerbaarheid

Onvoldoende inzicht in risico's en het ontbreken van een handelingsperspectief leiden ertoe dat bedrijven binnen het mkb niet weten waartegen ze zich precies moeten wapenen en welke cybermaatregelen zij moeten prioriteren als zij hun cyberweerbaarheid willen versterken. Uit onderzoek blijkt dat 50% van de bedrijven binnen het mkb geen risicoanalyses uitvoert en dus onvoldoende zicht heeft op cyberrisico's en het effect daarvan op de bedrijfsvoering[50]. Het gebrek aan inzicht in risico's en handelsperspectief maakt bedrijven binnen het mkb kwetsbaar en minder weerbaar tegen cyberaanvallen.

Daarnaast blijkt dat het maken van kwantitatieve inschattingen van risico's lastig is door een gebrek aan goede data. De tools die worden ontwikkeld om dit in kaart te brengen (bijvoorbeeld de toolkit voor het kwantificeren van cyberrisico's[51]) zijn vooral bruikbaar voor bedrijven met een hoog volwassenheidsniveau[52]. Veel bedrijven binnen het mkb hebben vaak niet het juiste volwassenheidsniveau om dit soort complexe tools toe te passen.

Daarnaast blijkt dat het management van bedrijven binnen het mkb niet altijd prioriteit geeft aan cyberweerbaarheid doordat zij vaak veel verschillende verantwoordelijkheden hebben[53]. Zo blijkt uit het Cyberweerbaarheid Onderzoek MKB Brabant dat bij slechts 50,8% van de respondenten van het onderzoek cyberweerbaarheid periodiek op de agenda van de directie staat[54]. Dit kan leiden tot het beperken van budgetten en middelen voor cybermaatregelen die inzicht in risico's en handelingsperspectief kunnen geven[55].

45 Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
46 CEOs' information security behavior in SMEs: does ownership matter?, Barlette et al. (2017)
47 Risk and the Small-Scale Cyber Security Decision Making Dialogue - an UK Case Study, Osborn & Simpson (2018)
48 Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
49 Nederlandse Cybersecuritystrategie 2022-2028, Rijksoverheid (2022)
50 Aanpak preventie cybercrime bij MKB, MKB-Nederland (2022)
51 Aan de slag met het kwantificeren van cyberrisico's, Nationaal Cyber Security Centrum (2020)
52 Kwantificering van cyberrisico's, Nationaal Cyber Security Centrum (2020)
53 Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
54 Cyberweerbaarheidsonderzoek MKB Brabant 2022, ACA IT-Solutions (2022)
55 Risk and the Small-Scale Cyber Security Decision Making Dialogue - an UK Case Study, Osborn & Simpson (2018)

Versterkende factoren
Een factor die onvoldoende inzicht in risico's en het ontbreken van een handelingsperspectief kan versterken is het gebrek aan cyberbewustzijn en -kennis, dit is een ander intern obstakel. Als bedrijven binnen het mkb niet bewust zijn van het feit dat cybersecurity een mogelijk risico is, gaan zij waarschijnlijk ook geen vervolgstappen nemen door deze cyberrisico's inzichtelijk te maken en te identificeren welke cybermaatregelen zij moeten nemen.

Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden

Het is lastig voor mkb'ers om in te schatten hoeveel en waarin geïnvesteerd moet worden. Dit is het derde interne obstakel dat bedrijven binnen het mkb ervaren in het behalen van een optimaal niveau van cyberweerbaarheid. Met 'hoeveel' wordt hier bedoeld dat het lastig is voor mkb'ers om in te schatten welke investeringshoogte passend is bij hun optimale cyberweerbaarheidsniveau. Met 'waarin' wordt hier bedoeld dat het lastig is voor mkb'ers welke ICT-oplossingen de juiste ICT-oplossingen zijn.

Al weten mkb'ers welk risico ze lopen en wat voor cybermaatregelen ze moeten nemen (handelingsperspectief), dan is er nog steeds een groot aantal ICT-oplossingen waaruit gekozen kan worden om te implementeren. Dit kan variëren van (geavanceerde) op maat gemaakt ICT-oplossingen tot simpele standaard ICT-oplossingen (zoals Two-Factor Authentication (2FA), back-ups, passwordmanagers). De kwaliteit en effectiviteit van de toepassingen is in het algemeen zeer lastig in te schatten door de ondernemer.

Impact op cyberweerbaarheid
Het feit dat het lastig is om de hoeveelheid en type investeringen in cyberweerbaarheid in te schatten kan ervoor zorgen dat bedrijven binnen het mkb onvoldoende investeren in het versterken van hun cyberweerbaarheid, terwijl er dikwijls wél voldoende financiële middelen voorhanden zijn. Daarnaast blijkt uit onderzoek dat bedrijven binnen het mkb (binnen dat onderzoek gedefinieerd als bedrijven met minder dan 100 miljoen omzet) beperkte schaalvoordelen hebben bij het investeren in cyberweerbaarheid omdat de potentiële schadevermindering van de investering onvoldoende rendabel is[56].

Kleinere bedrijven binnen het mkb hebben vaker beperkte financiële middelen tot hun beschikking waardoor ze een kleiner budget beschikbaar hebben voor cyberveiligheid en minder kunnen investeren in personeel met kennis over ICT en cyberveiligheid[57]. Daarnaast is bijvoorbeeld het gebruik van cyberverzekeringen niet altijd aantrekkelijk voor bedrijven binnen het mkb, doordat de premies vaak hoog zijn en zaken zoals de diefstal van intellectueel eigendom niet altijd zijn inbegrepen[58].

De grootte van een bedrijf, de omzet en het type ICT-oplossingen beïnvloeden de afwegingen die bedrijven binnen het mkb maken omtrent investeringen voor het versterken van hun cyberweerbaarheid[59].

Versterkende factoren
Twee factoren die het obstakel 'lastig te bepalen hoeveel en waarin geïnvesteerd moet worden' kunnen versterken zijn 'onvoldoende cyberbewustzijn en -kennis' en 'onvoldoende inzicht in risico en handelingsperspectief'. Beide factoren leiden tot een beperkt vermogen om überhaupt in te schatten welke cybermaatregelen moeten worden genomen. Dit is een belangrijke voorwaarde om te bepalen welke investeringshoogte en wat voor een type investeringen passend zijn bij het optimale cyberweerbaarheidsniveau van bedrijven binnen het mkb.

3.3.2 Externe obstakels

Algemeen tekort aan personeel in Nederland met expertise in ICT en cyberveiligheid

Een algemeen tekort aan personeel in Nederland met expertise in ICT en cybersecurity is het eerste externe obstakel dat bedrijven binnen het mkb ervaren in het behalen van een optimaal niveau van cyberweerbaarheid. Er is in Nederland een tekort aan personeel met expertise in zowel ICT als cyberveiligheid[60]. Dit tekort aan personeel beperkt ook bedrijven binnen het mkb in het nemen van cybermaatregelen om zichzelf te beschermen tegen cyberaanvallen.

Impact op cyberweerbaarheid
De schaarste in het aanbod van personeel resulteert in verhoogde tarieven voor de externe inhuur van experts[61]. Regelmatig maken bedrijven binnen het mkb daarom de afweging hier niet in te investeren wat hen hindert in het versterken van het cyberweerbaarheidsniveau.

Beperkte toepasbaarheid huidige cyberrichtlijnen voor het mkb

De beperkte toepasbaarheid van de huidige richtlijnen voor het mkb is het tweede externe obstakel dat bedrijven binnen het mkb ervaren in het behalen van een optimaal niveau van cyberweerbaarheid. In dit onderzoek wordt met een cyberrichtlijn een set van aanbevelingen bedoeld die beschrijven hoe bedrijven met het beveiligen van informatie kunnen omgaan, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie te waarborgen[62]. Voorbeelden van cyberrichtlijnen zijn de Algemene Verordening Gegevensbescherming (AVG) of de NIS2-richtlijn. De huidige cyberrichtlijnen bevatten vaak te algemene kaders en zijn opgesteld voor grotere bedrijven waar meer specialisatie mogelijk is. Daarnaast zijn deze richtlijnen vaak lastig te begrijpen zonder ondersteuning van cyberexperts[63].

56 Cyber Value at Risk in the Netherlands, Deloitte (2017)
57 Op weg naar een lokale aanpak voor digitale weerbaarheid bij het midden- en kleinbedrijf, Middelman (2022)
58 Cyber Value at Risk in the Netherlands, Deloitte (2017).
59 Informatie verkregen vanuit de klankbordgroep (2023)
60 "Nederlandse Cybersecuritystrategie (NLCS) 2022-2028: Ambities en acties voor een digitaal veilige samenleving", (2022)
61 De zoektocht naar ICT-personeel in een krappe arbeidsmarkt, Van Hout (2020)
62 Digitale Ethiek en veiligheid - Cybersecurity & Privacy - NEN
63 Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)

Impact op cyberweerbaarheid
Doordat de huidige cyberrichtlijnen niet altijd toepasbaar zijn voor bedrijven binnen het mkb, is het lastig voor deze bedrijven om inzicht te krijgen in welke cybermaatregelen zij dienen te implementeren. Hierdoor kan het zijn dat bedrijven binnen het mkb de verkeerde maatregelen implementeren of geen maatregelen implementeren wat een negatief effect heeft op de cyberweerbaarheid van deze bedrijven.

Afhankelijkheidsrisico's in de toeleveringsketen

Afhankelijkheidsrisico's in de toeleveringsketen en van ICT-leveranciers is het derde externe obstakel dat bedrijven binnen het mkb ervaren in het behalen van een optimaal niveau van cyberweerbaarheid. Het obstakel 'afhankelijkheidsrisico's in de toeleveringsketen' verwijst naar de risico's die ontstaan doordat bedrijven afhankelijk zijn van ketenpartners. Ketenpartners zijn personen of organisaties, buiten de eigen organisatie, die een bijdrage leveren aan de totstandkoming en of levering van het product of professioneel betrokken is bij het product of de klant[64].

Impact op cyberweerbaarheid
In veel gevallen zijn bedrijven binnen het mkb afhankelijk van de software, informatie, producten of services die geleverd worden door externe partijen.

Ten eerste kan het zo zijn dat deze externe partijen zelf kwetsbaar zijn voor cyberaanvallen en bedrijven binnen het mkb slachtoffer worden van cyberincidenten bij deze partijen. Zo wordt voorspeld dat in 2025 45% van de bedrijven wereldwijd te maken zullen hebben gehad met aanvallen op hun softwaretoeleveringsketens. Dit zou een drievoudige toename zijn ten opzichte van 2021[65].

Ten tweede besteden bedrijven binnen het mkb vaak ook hun cybersecuritymaatregelen uit aan externe partijen. Bedrijven binnen het mkb gaan er vaak vanuit dat de cybermaatregelen in de IT-producten die ze kopen voldoende zijn en dat er geen aanvullende cybermaatregelen nodig zijn, in de praktijk blijkt dit echter vaak niet zo te zijn. Daarnaast weten bedrijven binnen het mkb niet altijd of ze standaard of op maat gemaakte ICT-oplossingen moeten gebruiken; hierbij vertrouwen ze vaak volledig op hun ICT-leverancier. Bovendien blijkt dat kwaadwillenden zich steeds meer richten op cloudbedrijven, ICT-dienstverleners en softwareontwikkelaars[66].

Verder geldt dat bedrijven binnen het mkb zelf ook toeleveranciers kunnen zijn, en te maken kunnen krijgen met eisen rondom cyberveiligheid vanuit de klant. Indien meerdere klanten verschillende eisen stellen, kan het gebrek aan uniformiteit problemen veroorzaken voor de mkb'er.

Beperkte vindbaarheid van (overheids-)hulpmiddelen

Beperkte vindbaarheid van (overheids-)hulpmiddelen is het vierde externe obstakel dat bedrijven binnen het mkb ervaren in het behalen van een optimaal niveau van cyberweerbaarheid. De definitie '(overheids-)hulpmiddelen' verwijst in dit onderzoek specifiek naar informatievoorzieningen en hulpmiddelen die worden aangeboden om de cyberweerbaarheid van bedrijven binnen het mkb te versterken. Uit onderzoek blijkt dat bedrijven binnen het mkb vaak niet weten waar ze informatie en hulpmiddelen voor cyberweerbaarheid kunnen vinden[67]. Zo is slechts een kleine groep van de bedrijven binnen het mkb op de hoogte van het bestaan van het DTC, terwijl veel bedrijven juist wél aangeven behoefte te hebben aan de diensten die het DTC aanbiedt, zoals de 'Basisscan Cyberweerbaarheid'[68]. Hoewel er wel initiatieven zijn opgestart om de bekendheid te verbeteren, bijvoorbeeld door middel van de invoering van het landelijk dekkend stelsel informatieknooppunten, zijn er nog steeds bedrijven binnen het mkb die onvoldoende op de hoogte zijn van waar ze terecht kunnen met vragen of problemen omtrent cyberveiligheid[69].

Impact op cyberweerbaarheid
Bedrijven binnen het mkb die een suboptimaal cyberweerbaarheidsniveau hebben, zijn gebaat bij hulpmiddelen die vanuit de overheid worden aangeboden om hun cyberweerbaarheid te versterken. Een hulpmiddel is in deze context een niet-commercieel middel dat een bedrijf binnen het mkb kan helpen hun cyberweerbaarheid te versterken (voor meer informatie over de definitie van een hulpmiddel zie hoofdstuk 4. Overzicht huidige hulpmiddelen). Door de grote hoeveelheid hulpmiddelen en het gebrek aan samenhang tussen de hulpmiddelen weten bedrijven binnen het mkb vaak niet waar ze de juiste hulpmiddelen kunnen vinden en wat de juiste hulpmiddelen voor hen zijn. Hierdoor gebruiken ze de hulpmiddelen niet. Dit hindert de bedrijven in het verbeteren van hun cyberweerbaarheid[70].

Veranderend dreigingslandschap

Het steeds veranderende dreigingslandschap is het vijfde externe obstakel dat bedrijven binnen het mkb ervaren in het behalen van een optimaal niveau van cyberweerbaarheid. Het dreigingslandschap verwijst naar dreigingen in het digitale domein[71].

64 https://www.encyclo.nl/begrip/ketenpartners
65 Strategic Roadmap to building a World Class software engineering Organization, Gartner (z.d.)
66 PrivacyWaakhond: Veel meer datalekken door cyberaanvallen gemeld, Wilman (2022)
67 Informatie-uitwisseling landelijk dekkend stelsel, Brennenraedts et al. (2020)
68 Informatie verkregen vanuit de klankbordgroep (2023)
69 Nationaal Cyber Security Centrum (2023)
70 Informatie verkregen vanuit de klankbordgroep (2023)
71 Het NCSC en dreigingsinformatie, Nationaal Cyber Security Centrum (2021)

Sinds het begin van de COVID-19 crisis is er een aanzienlijke toename geweest in het gebruik van digitale dienstverlening en outsourcen bedrijven binnen het mkb vaker hun ICT-oplossingen. Deze ontwikkeling heeft echter ook geleid tot een vergroting van de 'attack surface' (aanvalsoppervlak). Parallel zijn veranderingen in het dreigingslandschap aangewakkerd door de voortdurende ontwikkeling van geavanceerde technieken en -methoden voor cyberaanvallen. Cybercriminelen passen zich voortdurend aan om nieuwe kwetsbaarheden en zwakke plekken in beveiligingssystemen te exploiteren.

Impact op cyberweerbaarheid
Het is lastig voor bedrijven binnen het mkb om hun digitale infrastructuur volledig af te stemmen op de steeds meer geavanceerde cyberdreigingen. Dit geldt met name voor bedrijven binnen het mkb die op maat gemaakte ICT-oplossingen gebruiken. Een mkb'er die gebruik maakt van standaard oplossingen (zoals Microsoft Office 365) zal er minder last van hebben omdat ICT-leveranciers vaak zelf patches uitvoeren voor hun producten. Echter ben je als gebruiker nog wel verantwoordelijk om deze producten zelf te updaten en kan het zijn dat je als gebruiker alsnog aanvullende maatregelen moet nemen om beter beschermd te zijn tegen veranderende dreigingen.

Technologische trends en ontwikkelingen spelen hierbij een rol: nieuwe technologieën creëren nieuwe potentiële ingangen voor aanvallers om toegang te krijgen tot systemen en gegevens. Deze technologische evolutie vereist voortdurende aanpassingen in beveiligingsstrategieën om nieuwe dreigingen het hoofd te bieden[72]. Het is een uitdaging voor bedrijven binnen het mkb (die op maat gemaakte ICT-oplossingen gebruiken) om bij te blijven met de nieuwste dreigingsinformatie, -trends en -tactieken[73]. Dit kan een negatieve impact hebben op de cyberweerbaarheid van bedrijven binnen het mkb.

[72] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[73] Informatie verkregen vanuit de klankbordgroep (2023))

4. Overzicht huidige hulpmiddelen

4. Overzicht huidige hulpmiddelen

4.1 Introductie

In dit hoofdstuk wordt een inventarisatie gemaakt van de hulpmiddelen die bedrijven binnen het mkb kunnen gebruiken om hun cyberweerbaarheid te verbeteren. Het betreft hier uitdrukkelijk geen volledig overzicht van alle beschikbare hulpmiddelen.
Het overzicht bestaat uit hulpmiddelen die relatief eenvoudig vindbaar kunnen zijn voor mkb-bedrijven. In de praktijk zijn er meer hulpmiddelen beschikbaar. Voor het onderzoek is deze inventarisatie gedaan om op hoofdlijnen inzicht te kunnen krijgen in beschikbare hulpmiddelen en de bijdrage die ze zouden kunnen leveren in het wegnemen van obstakels.

4.1.1 Doel van de inventarisatie

Het creëren van een overzicht van de bestaande hulpmiddelen is de eerste stap in het komen tot een conclusie over de effectiviteit van de hulp die geboden wordt, vanuit het publieke en private domein, aan de bedrijven binnen het mkb. Evaluatie van de hulpmiddelen wordt gedaan per hulpmiddelen categorie en niet per individueel hulpmiddel. Dit wordt beschreven in hoofdstuk 5. Stimuleren en verbeteren'.

4.1.2 Definitie hulpmiddel

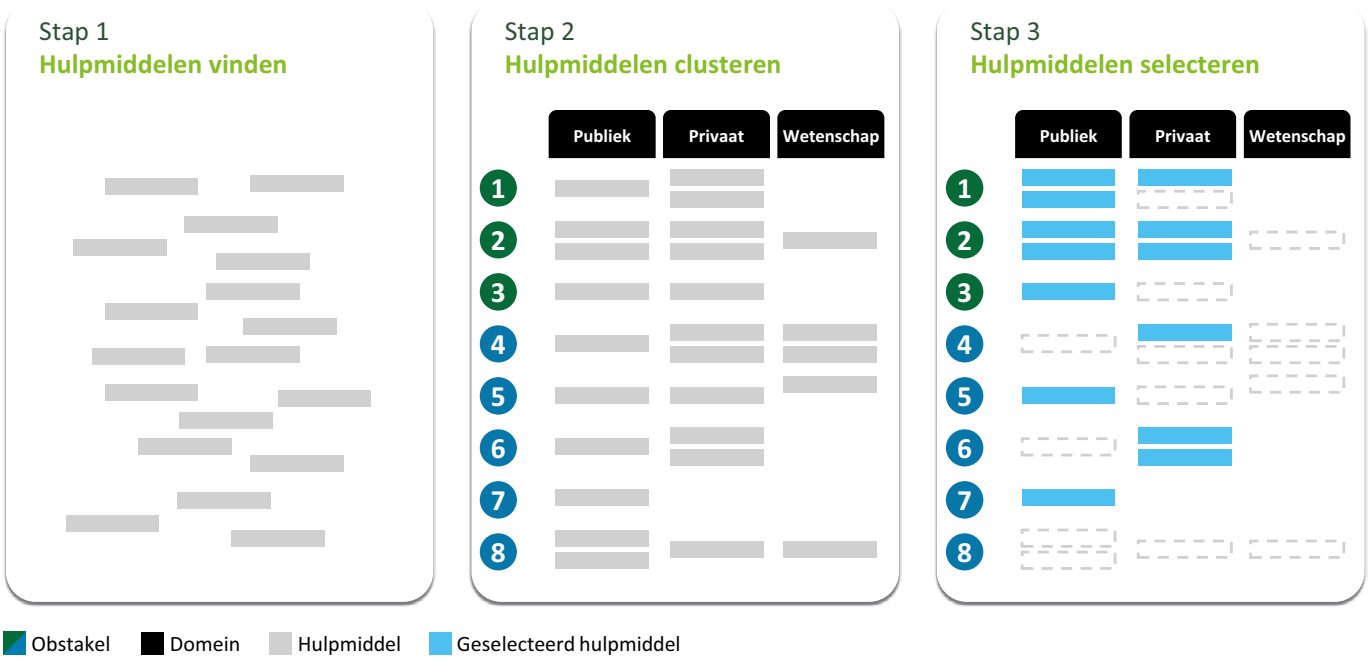
In dit onderzoek omvat het begrip 'hulpmiddelen' alle niet-commerciële middelen die bedrijven binnen het mkb in Nederland kunnen helpen hun cyberweerbaarheid te versterken, gegeven hun risicoprofiel en (beoogd) volwassenheidsniveau. Onder dit begrip vallen verschillende typen hulpmiddelen, zoals: het in kaart brengen van het cyberweerbaarheidsniveau van een bedrijf door middel van een gratis, online zelf-scan aan de hand van een lijst met vragen, of het aanzetten tot handelen door middel van een webpagina met cyberveiligheidsbasismaatregelen.

4.2 Aanpak inventarisatie hulpmiddelen

Het overzicht aan hulpmiddelen is gesplitst in twee tabellen. De eerste tabel (zie Tabel 4) bevat 64 algemene hulpmiddelen, waar iedereen vrij toegang toe heeft. De tweede tabel (zie Tabel 12 in Appendix D – Overzicht samenwerkingsverbanden) bevat 187 hulpmiddelen aangeboden door 51 van de totaal 58 samenwerkingsverbanden. Een samenwerkingsverband is een cyberweerbaarheidsnetwerk waar ondernemers samen met andere organisaties samenwerken aan het vergroten van de cyberweerbaarheid, binnen en tussen branches, sectoren en regio's. Voor dit overzicht aan hulpmiddelen is het overzicht aan cyberweerbaarheidsnetwerken gebruikt waarmee het DTC samenwerkt[74].

4.2.1. Aanpak inventarisatie algemene hulpmiddelen

Om te komen tot het overzicht aan algemene hulpmiddelen zijn drie stappen doorlopen (zie Figuur 3).



Figuur 3 Aanpak inventarisatie algemene hulpmiddelen.

[74] Overzicht van samenwerkingsverbanden, DTC

Stap 1: hulpmiddelen vinden

Door middel van deskresearch is een overzicht gemaakt van ruim 90 hulpmiddelen. Het bestaan van een hulpmiddel betekent overigens niet zonder meer dat deze ook effectief is in het oplossen van een obstakel. Dit overzicht is besproken met de leden van de klankbordgroep en tijdens de interviews met de mkb'ers en waar mogelijk aangevuld.

Stap 2: hulpmiddelen clusteren

De gevonden hulpmiddelen zijn geclusterd langs twee assen: obstakels en domeinen. In hoofdstuk 3 zijn in totaal acht interne en externe obstakels gedefinieerd die bedrijven binnen het mkb ondervinden in het versterken van hun cyberweerbaarheid. De koppeling met de obstakels geeft aan welk probleem het hulpmiddel dient te verhelpen. Zo kan inzichtelijk worden gemaakt of de beschikbare hulpmiddelen aansluiten bij de behoeftes van bedrijven binnen het mkb. De koppeling met de obstakels is gedaan op basis van het primaire doel van het hulpmiddel. Het kan zijn dat sommige hulmiddelen indirect ook bijdragen aan het oplossen van andere obstakels. Zo draagt bijvoorbeeld een risicoanalyse ook bij aan het verhogen van cyberbewustzijn en -kennis. Deze indirecte relatie is niet meegenomen in het onderzoek om zo duidelijk in kaart te kunnen brengen waar de hiaten liggen (i.e. voor welke obstakels nog onvoldoende hulpmiddelen worden aangeboden of waar hulpmiddelen nog niet effectief zijn).

De koppeling met de twee domeinen (publiek, privaat) geeft aan wie de aanbieder is van het hulpmiddel. Hier wordt onderscheid gemaakt tussen:

- **Publiek.** Dit domein omvat alle publieke instellingen en non-profitorganisaties die gelinkt zijn aan de overheid of namens de overheid taken uitvoeren.
- **Privaat.** Dit domein omvat particuliere bedrijven en organisaties en met name particuliere verenigingen en stichtingen zonder winstoogmerk. Het kan wel zijn dat private partijen subsidies ontvangen vanuit de overheid.

De hulpmiddelen aangeboden vanuit het wetenschappelijke domein voldoen niet aan de selectiecriteria en zijn daarom niet meegenomen in Tabel 4.

Stap 3: hulpmiddelen selecteren

Om te komen tot een overzicht aan hulpmiddelen die aansluiten bij de behoeftes van bedrijven binnen het mkb en aanzetten tot handelen, zijn vier selectiecriteria opgesteld. Hierbij geldt dat een hulpmiddel alleen geselecteerd wordt als deze voldoet aan criteria 1A, of 1B, of 1C, én 2 én 3. De criteria zijn als volgt gedefinieerd:

1. A. Het hulpmiddel is expliciet gericht op bedrijven binnen het mkb

Dit betekent dat de betreffende hulpmiddelen afgestemd zijn op bedrijven binnen het mkb. In tegenstelling tot sommige generieke hulpmiddelen, helpen deze hulpmiddelen specifiek bij het optimaliseren van de cyberweerbaarheid van bedrijven binnen het mkb.

Voorbeeld

- Hulpmiddel dat niet voldoet aan criterium 1A: het jaarlijkse Cybersecuritybeeld van Nederland dat gepubliceerd wordt in een rapport van de NCTV; deze biedt inzicht in de strategische cybersecuritythema's voor de Nederlandse Cybersecurity strategie en focust niet specifiek op bedrijven binnen het mkb.
- Hulpmiddel dat wel voldoet aan criterium 1A: subsidie 'Mijn cyberweerbare zaak', gericht op bedrijven met maximaal 50 werknemers en € 10 miljoen omzet.

B. Het hulpmiddel wordt aangeboden of aangeraden door een partij die zich richt op bedrijven binnen het mkb

Een hulpmiddel dat wordt aangeboden of aangeraden door een partij die zich richt op de cybergerelateerde behoeftes, uitdagingen en doelstellingen van bedrijven binnen het mkb. Dit benadrukt de relevantie en de toepasbaarheid van de hulpmiddelen voor bedrijven binnen het mkb.

Voorbeeld

- Hulpmiddel dat niet voldoet aan criterium 1B: rapport 'Samenhangend Inspectiebeeld Cybersecurity Vitale Processen 2023' van een groep Nederlandse toezichthouders.
- Hulpmiddel dat wel voldoet aan criterium 1B: het Agrifood Cybersecurity Self Assessment (AgroConnect).

C. Het hulpmiddel is relevant of waardevol voor bedrijven binnen het mkb

Dit zijn hulpmiddelen die niet expliciet gericht zijn op bedrijven binnen het mkb, én niet worden aangeboden door een partij die zicht richt op bedrijven binnen het mkb, maar wel relevant of waardevol kunnen zijn voor deze bedrijven.

Voorbeeld

- Hulpmiddel dat niet voldoet aan criterium 1C: Nederlandse Cyber Security Onderzoek Agenda van het NCSC.
- Hulpmiddel dat wel voldoet aan criterium 1C: Overheidsbreed Cyberprogramma (BZK).

2. Het hulpmiddel is geen commerciële dienst van een private partij

Individuele, bestaande hulpmiddelen van commerciële partijen met een winstoogmerk worden niet meegenomen in de inventarisatie naar hulpmiddelen. Dit laat onverlet dat private partijen waardevolle hulpmiddelen kunnen aanbieden voor het mkb. De markt heeft namelijk een grote capaciteit en een sterk innovatievermogen dat kan leiden tot betaalbare oplossingen. Verder is de rol van de overheid ook wettelijk begrensd om marktverstoring te voorkomen.

Voorbeeld

- Hulpmiddel dat niet voldoet aan criterium 2: cyberverzekeringen van private partijen.
- Hulpmiddel dat wel voldoet aan criterium 2: infoblad 'Afsluiten cyberverzekering' van de Kamer van Koophandel (KVK).

3. Het hulpmiddel vereist geen vergevorderde kennis omtrent cyberweerbaarheid

Het hulpmiddel vereist geen vergevorderde kennis omtrent cyberweerbaarheid om effectief gebruikt te kunnen worden. Dit betekent dat het ontworpen is met het oog op gebruiksgemak en toegankelijkheid voor bedrijven binnen het mkb, die soms niet beschikken over diepgaande kennis en expertise op het gebied van cyberweerbaarheid.

Voorbeeld

- Hulpmiddel dat niet voldoet aan criterium 3: Factsheet Open Source Security; dit is een hulpmiddel dat wordt aangeboden vanuit het NCSC en focust op Software Supply Chain Security en Open Source, wat een bepaalde mate van cyberkennis vraagt.
- Hulpmiddel dat wel voldoet aan criterium 3: Toolbox Cyberincident met een stappenplan aangeboden door de Digitale Overheid.

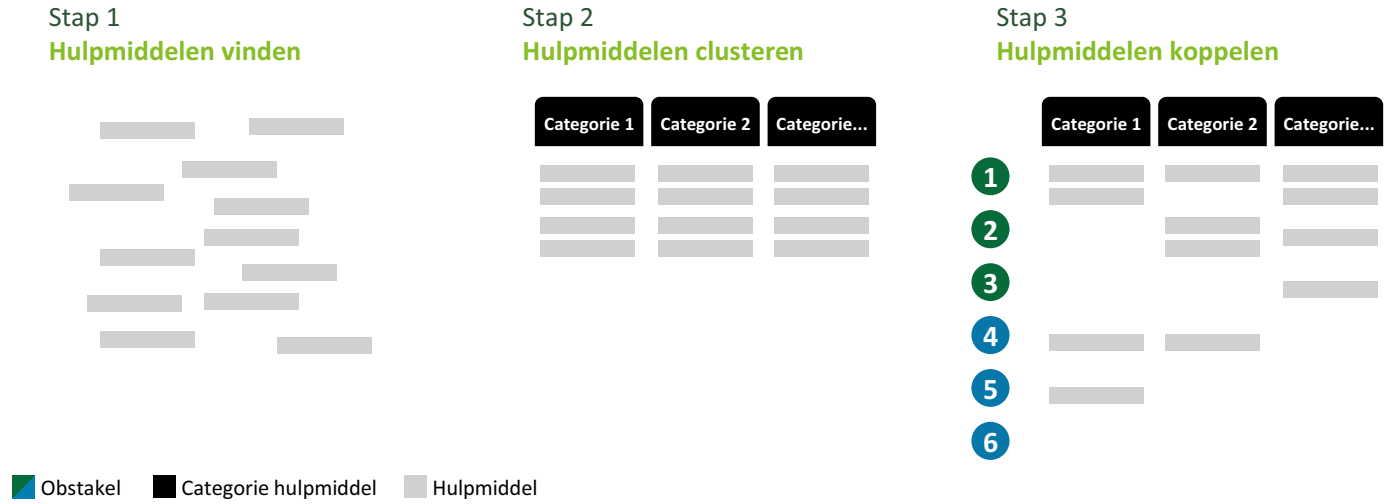
4.2.2. Aanpak hulpmiddelen samenwerkingsverbanden

Om te komen tot het overzicht aan hulpmiddelen vanuit de samenwerkingsverbanden zijn drie stappen doorlopen (zie Figuur 4).

Stap 1: hulpmiddelen vinden

Voor het creëren van een overzicht aan hulpmiddelen aangeboden vanuit cyberweerbaarheidsnetwerken is het overzicht aan samenwerkingsverbanden vanuit het DTC gebruikt. Het DTC noemt 58 unieke samenwerkingsverbanden, en geeft per samenwerkingsverband aan welke activiteiten aangeboden worden. Van deze 58 zijn er 51 meegenomen in dit onderzoek; de resterende 7 samenwerkingsverbanden voldoen niet geheel aan de selectiecriteria. Een voorbeeld hiervan is het CIP die zich richt op de overheid en niet het mkb. De 51 partijen bieden gezamenlijk 187 hulpmiddelen aan (zie Tabel 12 in Appendix D – Overzicht samenwerkingsverbanden). Belangrijk om te noemen:

- Dit overzicht aan hulpmiddelen is niet compleet gezien dit enkel de hulpmiddelen zijn van cyberweerbaarheidsnetwerken waar het DTC mee samenwerkt.
- De definitie van een 'hulpmiddel' heeft invloed op het totale aantal hulpmiddelen. Voor dit onderzoek is bijvoorbeeld het organiseren van bijeenkomsten geduid als een enkel hulpmiddel, ongeacht hoeveel bijeenkomsten er worden georganiseerd.



Figuur 4 Aanpak inventarisatie hulpmiddelen.

Stap 2: hulpmiddelen clusteren
In deze stap zijn de 187 hulpmiddelen geclusterd in 11 categorieën hulpmiddelen. De categorisering is als volgt gemaakt (Tabel 3):

Categorie hulpmiddel	Voorbeelden
Bijeenkomst voor kennisdeling en bewustwording	Symposium, masterclass, deepdive, themasessie, training, meetup, webinar, cursus, workshop, werkgroep
Schriftelijke kennisdeling en voorlichting	Nieuwsbericht, praktische handvatten, nieuwsbrief, kennisbank, toolbox, cybernoodplan, stappenplan, checklist, publicatie, rapportage, whitepaper, template, dashboard, framework, servicedocument
Database ICT-leveranciers	Cyberweerbaarheidsregister, zoekmachine
Cybertools en -maatregelen, gratis of tegen gereduceerde prijs	Pentesten, basis cyberweerbaarheidsscan, nulmeting, platform met realtime risico's
Analyseren en delen van (acute) dreigingsinformatie voor handelingsperspectief	Cyberincidenten, cyberdreigingen, monitoring, bewaking
Meldpunt en noodhulplijn	Meldpunt voor IT-storingen
Professioneel advies en begeleiding	Digitaal loket, herstel na incident
(Cyber)crisisoefening	Jaarlijkse crisisoefening, oefenscenario's, cyberoefeningen
Certificaten en keurmerken	CYRA certificering, thuiswinkel waarborg certificering e-commerce
Voorlichtingscampagne	Hackshield campagne, online orde, re-BOOTCMP
Cyberverzekering	Verzekering tegen cyberrisico's vanuit het samenwerkingsverband geïnitieerd

Tabel 3 Voorbeelden van de verschillende categorieën hulpmiddelen.

Stap 3: hulpmiddelen koppelen
Als laatste stap zijn de hulpmiddelen gekoppeld aan een van 8 geïdentificeerde obstakels. Dit om in kaart te brengen op welke problemen deze cyberweerbaarheidsnetwerken zich voornamelijk richten, en met welk type hulpmiddel. Een themasessie rondom cybersecurity is bijvoorbeeld gekoppeld aan obstakel 1 'onvoldoende cyberbewustzijn en -kennis'.

Verantwoording volledigheid overzicht hulpmiddelen
Het overzicht van hulpmiddelen (zowel algemene hulpmiddelen als wel hulpmiddelen vanuit de samenwerkingsverbanden) is opgesteld op basis van deskresearch, gesprekken met de klankbordgroep en experts binnen dit gebied. Echter, de volledigheid van het overzicht kan niet gegarandeerd worden als gevolg van het feit dat hulpmiddelen niet altijd even makkelijk vindbaar zijn mede door de grote diversiteit aan aanbieders en bronnen.

4.3 Overzicht geselecteerde hulpmiddelen

	Domein		
Obstakel	**Publiek**	**Privaat**	**#**
1 Onvoldoende cyberbewustzijn en -kennis	• Alert Online (EZK) • Overheidsbreed Cyberprogramma (BZK)	• NLSecure[ID] conferentie (KPN) • CyberSecurityBooster (IWS, MKB Cybercampus, DTC, PVO Limburg)	**4**
2 Onvoldoende inzicht in risico's	• Risicoklasse Tool (DTC) • Security Check Procesautomatisering (DTC)	• Agrifood Cybersecurity Self Assessment (AgroConnect) • Risicoanalyse voor informatiebeveiliging (RAVIB)	**4**
Onvoldoende inzicht in handelingsperspectief	**Cyberweerbaarheidsniveau in kaart brengen: (7)** • Update Test (DTC) • Basisscan Cyberweerbaarheid (DTC) • CyberVeilig Check (DTC) • Back-up Test (DTC) • SME Cloud Security Tool (ENISA) • Cyber Security Healthcheck (CSR) • Zelf-evaluatie NIS2 (RDI) **Informatie en stappenplannen: (14)** • Webpagina basismaatregelen cybersecurity (NCSC) • Starten met 7 cybersecurity maatregelen (DTC) • Webpagina cybersecurity (Digitale Overheid) • Diverse handreikingen, zoals 'Start een ketensamenwerking' (NCSC) • veiliginternetten.nl (EZK, NCSC, ECP) • Informatie en advies rondom cyberverzekeringen (DTC) • Veilig online (Autoriteit Consument & Markt) • Toolbox Cyberincident (Digitale Overheid) • Cybersecurity: de basis (KVK) • Artikelen, tips, en video's over diverse cyberonderwerpen (KVK) • Infoblad afsluiten cyberverzekering (KVK) • Basismaatregelen veilig zakendoen (KVK) • Digitale veiligheid bespreken met IT-dienstverlener (DTC) • No More Ransom (Nationale Politie) **Kennisdeling: (3)** • DTC Community (DTC) • LinkedIn pagina 'Cybernetwerk Ondernemend Nederland' (KVK) • Start Event 'Veilig online ondernemen' (KVK) **Delen van dreigingsinformatie: (1)** • Waarschuwingsservice bij ernstige cyberdreiging (DTC) **Meldpunt en deskundig advies: (3)** • Aangiftepunt cybercrime (Nationale Politie) • Hackhelpdesk (DTC, Nationale Politie) • Chatbot en adviesteam voor ondernemersvragen (KVK)	**Cyberweerbaarheidsniveau in kaart brengen: (1)** • Testtool Internet.nl (Platform Internetstandaarden) **Incident response oefeningen: (1)** • Cyber Chain Resilience Consortium (ECP, DTC) **Informatie en stappenplannen: (7)** • Calamiteitenplan (MKB Cyber Campus) • Maak je eigen Cyber Incident Response Plan (Stichting Internet Domeinregistratie Nederland) • Cybernoodplan (MKB Nederland) • Webpagina Cybercrime (CCV) • Webpagina 'De NIS2 wet' (Samen Digitaal Veilig) • HSD Financieringswijzer (Security Delta) • NLdigital Kennisbank (NLdigital) **Kennisdeling: (4)** • Webinars met informatie en advies over digitale veiligheid (Samen Digitaal Veilig) • Webinars, podcasts, blogs en rapporten via Security Insight (Security Delta) • MKB DigiCafé (Security Delta, MKB Digiwerkplaatsen, IT Campus Rotterdam, Dutch Innovation Factory) • Themabijeenkomsten, workshops en podcasts (CIP) **Helpdesk: (1)** • Fraudehelpdesk (Stichting Aanpak Financieel-Economische Criminaliteit Nederland) **Overig: (3)** • Security Framework for Small Medium Enterprises (Small and Medium-sized Enterprises Security) • Cybersecurity woordenboek (Cyberveilig Nederland) • Veiligheidsdashboard (Samen Digitaal Veilig)	**45**
3 Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden	• Subsidieregeling Cyberweerbaarheid (RVO) • Mijn cyberweerbare zaak (RVO) • Diverse sancties voor het overtreden van privacywetgeving (Autoriteit Persoonsgegevens)		**3**
4 Algemeen tekort aan personeel met expertise in cyber en ICT		• cybersecuritywerkt.nl voor advies en informatie over omscholing (Security Delta)	**1**
5 Beperkte toepasbaarheid huidige cyberrichtlijnen voor het mkb	• Stappenplan: AVG op orde voor ondernemers en mkb (Autoriteit Persoonsgegevens) • Webpagina NIS2-richtlijn (Digitale Overheid)		**2**
6 Afhankelijkheidsrisico's in toeleveringsketen	• Afspraken maken met een IT-leverancier (DTC)	**Certificeringen: (2)** • Keurmerk voor ICT-dienstverleners (CCV) (In ontwikkeling) • CYRA Cyber Rating (CW Brainport, FERM Rotterdam, MKB Cyber Campus, ASML, TÜV Nord Nederland) **Groot-helpt-klein principe: (1)** • Voorbeeld: CISO Circle of Trust (ASML)	**4**
7 Beperkte vindbaarheid van (overheids-)hulpmiddelen	• Wegwijzer voor Cybersecurity Initiatieven (DTC)		**1**
8 Veranderend dreigingslandschap			**0**
Aantal hulpmiddelen (#)	**39**	**25**	**64**

Tabel 4 Overzicht geselecteerde algemene hulpmiddelen.

4.4 Observaties algemene hulpmiddelen

In deze sectie zijn observaties weergegeven die voort zijn gekomen uit het onderzoek naar de hulpmiddelen. Een observatie in deze context is een objectieve, neutrale waarneming die kan leiden tot het opstellen en valideren van hypotheses over bijvoorbeeld de beschikbaarheid of effectiviteit van hulpmiddelen in latere hoofdstukken.

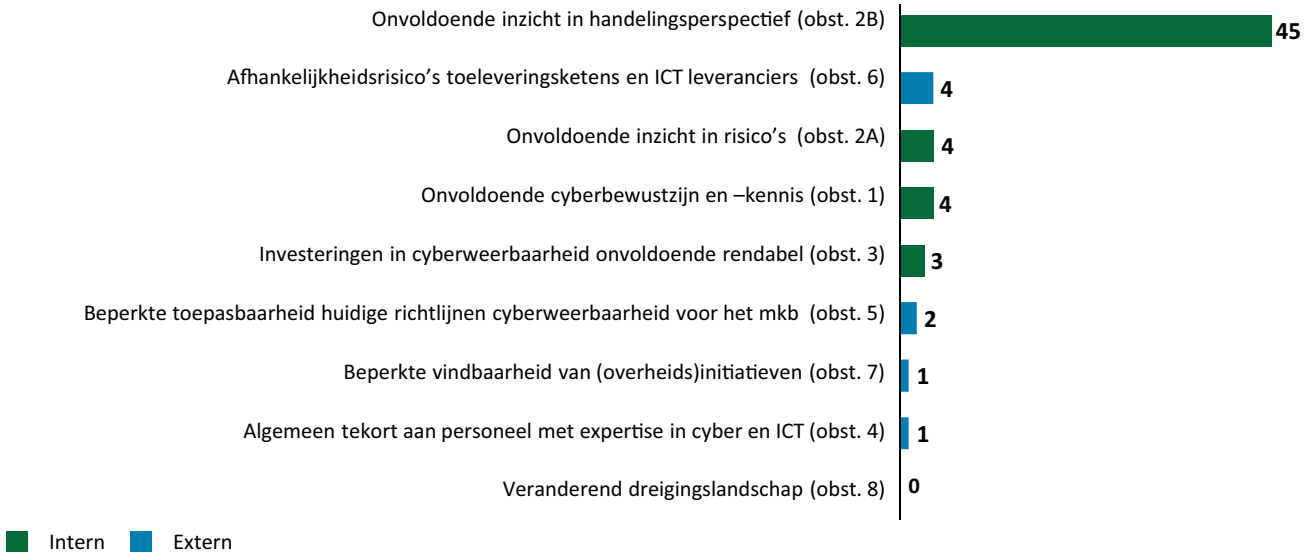
In het overzicht van de hulpmiddelen kunnen hiaten worden geïdentificeerd. Dit zijn ofwel obstakels waarvoor weinig hulpmiddelen beschikbaar zijn, of domeinen van waaruit weinig hulpmiddelen aangeboden worden. Op basis hiervan kunnen niet direct conclusies getrokken worden, gezien het feit dat een enkel hulpmiddel effectiever kan zijn dan tien andere, maar het biedt wel input voor verdere verdieping.

De observaties zijn geclusterd aan de hand van de obstakels.

4.4.1 Observaties met betrekking tot de obstakels

Verdeling over de obstakels

De verdeling van de 64 hulpmiddelen over de acht obstakels is weergegeven in Figuur 5.



Figuur 5 Verdeling van de hulpmiddelen over de obstakels.

Figuur 5 laat zien dat ongeveer driekwart (45 van de in totaal 64) van de geselecteerde hulpmiddelen gekoppeld zijn aan obstakel 2B en dus gericht zijn op het creëren van inzicht in handelingsperspectief voor bedrijven binnen het mkb.

Inzicht in risico's en handelingsperspectief

Er zijn in totaal drie hulpmiddelen die inzicht bieden in de risico's dat een bedrijf loopt, waarvan de Risicoklasse Tool van het DTC de meest uitgebreide en algemene is.
Bij het bieden van handelingsperspectief door middel van toolboxen of cybermaatregelen wordt er niet per definitie rekening gehouden met de belangrijkste risico's van een bedrijf. Een deel van de cybermaatregelen geldt voor ieder bedrijf en valt onder de 'basishygiëne' (bijvoorbeeld het maken van back-ups) maar een aantal meer geavanceerde maatregelen is afhankelijk van het risicoprofiel van de organisatie. Indien de hulpmiddelen hier geen inzicht in bieden, wordt het dus lastig voor bedrijven binnen het mkb om te bepalen welke maatregelen zij moeten prioriteren.

Wat opvalt is dat, hoewel tools zoals de Risicoklasse Tool bestaan, er in verhouding ruim 11 keer zoveel hulpmiddelen zijn die inzicht moeten bieden in handelingsperspectief, vergeleken met hulpmiddelen gericht op het in kaart brengen van risico's.

Investeren in cybermaatregelen

Hulpmiddelen voor obstakel 3 'Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden' kunnen ingedeeld worden in twee categorieën:

- Middelen die gericht zijn op de inkomsten van een bedrijf; denk bijvoorbeeld aan subsidies die financiële ondersteuning bieden voor het aanschaffen van cyberweerbaarheidsmaatregelen.
- Middelen die gericht zijn op de uitgaven van een bedrijf; denk bijvoorbeeld aan het opleggen van boetes bij het niet of verkeerd navolgen van wet- en regelgeving.

Er zijn op dit moment twee verschillende subsidies beschikbaar voor bedrijven binnen het mkb: Subsidieregeling Cyberweerbaarheid (RVO) en Mijn Cyberweerbare zaak (RVO). Deze worden beide tijdelijk aangeboden voor een periode van één tot anderhalve maand. Sancties worden op dit moment met name gegeven vanuit het overtreden van privacywetgeving zoals de AVG vanuit de Autoriteit Persoonsgegevens.

Beperkte toepasbaarheid van cyberrichtlijnen voor het mkb
Er zijn hulpmiddelen gericht op het helpen van bedrijven rondom bijvoorbeeld de verantwoordingsplicht vanuit de Algemene Verordening Gegevensbescherming (AVG; zie hulpmiddel 'AVG stappenplan' van de Autoriteit Persoonsgegevens), maar concrete, praktische standaarden voor bedrijven binnen het mkb rondom de aankomende NIS2 zijn niet gevonden. Een reden hiervoor is dat de tekst van de nationale wetgeving voor NIS2 nog niet in consultatie is gegaan.

Het lectoraat Cyber Security van de Hogeschool Utrecht is wel een praktische standaard aan het ontwikkelen voor mkb-bedrijven om zich beter te kunnen beveiligen tegen cybercriminaliteit, maar deze standaard is nog in ontwikkeling.[75]

Afhankelijkheidsrisico's
Er zijn twee typen hulpmiddelen geïdentificeerd die als doel hebben de afhankelijkheidsrisico's in de toeleveringsketen te mitigeren. Het eerste type hulpmiddel is 'certificeringen en keurmerken'. Er zijn geen certificeringen of keurmerken gevonden die specifiek gericht zijn op bedrijven binnen het mkb. Er is één keurmerk voor ICT-dienstverleners in ontwikkeling vanuit het CCV. Dit keurmerk zal inzicht bieden aan mkb-organisaties in de mate waarin de basismaatregelen voor cyberveiligheid worden nageleefd door hun ICT-dienstverleners. Verder is er het keurmerk de CYRA Cyber Rating; deze wordt al veelvuldig gebruikt door (grotere) organisaties, maar nog niet (veel) door bedrijven binnen het mkb.

Het tweede type hulpmiddel is het 'groot-helpt-klein' principe waarbij een groter, meer cybervolwassen bedrijf in de waardeketen leveranciers (vaak kleinere bedrijven) helpt of zelfs verplicht tot het versterken van de cyberweerbaarheid vanwege de onderlinge afhankelijkheidsrisico's. Een voorbeeld hiervan is de 'CISO Circle of Trust (CCoT)'[76], opgericht in 2022 door tien Nederlandse bedrijven (Rabobank, NS, KPN, ABN AMRO, Philips, ING, Ahold Delhaize, ASML, Shell, AkzoNobel). Deze stichting heeft als doel de leden, maar uiteindelijk ook bedrijven daarbuiten, weerbaarder te maken tegen cyberaanvallen en -incidenten. De CISO Circle of Trust heeft onlangs de OKTT-status (zie 4.4.1 – 'Veranderd dreigingslandschap' voor meer informatie) ontvangen[77], wat betekent dat het wettelijk toegestaan is voor het NCSC om dreigingsinformatie te delen met de stichting, die deze informatie weer kan delen met de bij de Circle of Trust aangesloten partijen en daarbuiten met bedrijven in (cross)sectorale ketens[78].

Verder noemt het DTC dat de Circle of Trust een aanbeveling heeft ontwikkeld voor 26 security controls, gericht op bedrijven binnen het mkb die een start willen maken met hun cyberweerbaarheid. Hiervan is onduidelijk in hoeverre dit hulpmiddel gebruikt wordt en wat de effectiviteit is.

Beperkte vindbaarheid van (overheids-)hulpmiddelen
Dit obstakel is een overkoepelend probleem omdat het gezien kan worden als een voorwaarde voor het implementeren van (overheids-)hulpmiddelen. Als een hulpmiddel beperkt vindbaar is, wordt er ook beperkt gebruik van gemaakt, wat een negatieve invloed heeft op de effectiviteit van het hulpmiddel. Het enige hulpmiddel dat is gevonden dat als primair doel heeft het beter vindbaar maken van andere hulpmiddelen, is de 'Wegwijzer voor Cybersecurity Initiatieven' van het DTC. Dit is een online overzicht van 51 cyberveiligheidsinitiatieven, inclusief omschrijving en verwijzing naar relevante websites. Ook is er een zoekmachine voor het filteren van initiatieven, afhankelijk van bijvoorbeeld het benodigde cyberkennisniveau.

Veranderend dreigingslandschap
Voor obstakel 8 (Veranderend dreigingslandschap) zijn er geen hulpmiddelen gevonden die door de selectiecriteria heen komen. Een voorbeeld hiervan is het Landelijk Dekkend Stelsel Informatieknooppunten (LDS) van de NCTV[79,80]. Dit is een systeem waarbij informatie over digitale dreigingen en kwetsbaarheden vanuit bijvoorbeeld het NCSC, de AIVD, MIVD, Politie, OM, etc., verzameld, verwerkt en verspreid wordt. Het is mogelijk voor bedrijven binnen het mkb om deze informatie te ontvangen. Daarnaast kunnen bedrijven deze informatie ontvangen als ze zijn aangesloten bij een van de CERT's (Computer Emergency Response Team, zoals de Z-CERT voor zorginstellingen) of een van de OKTT's (Objectief Kenbaar Tot Taak, zoals bijvoorbeeld FERM in de Rotterdamse haven). OKTT's zijn schakelorganisaties die als taak hebben informatie door te spelen naar aangesloten partijen. Een ander voorbeeld hiervan is het DTC dat als schakelorganisatie dient voor het niet-vitale bedrijfsleven (zie het DTC voor meer informatie hierover)[81]. Het LDS is dus niet per definitie gericht op bedrijven binnen het mkb. Indien de informatie via de juiste partijen wordt aangeboden en schaalbaar is voor het mkb, zou dit hulpmiddel wel relevant kunnen zijn voor bedrijven binnen het mkb.

[75] HU gaat cybersecurity toepasbaar maken voor kleinere bedrijven en organisaties, Hogeschool Utrecht (2023)
[76] CISO Circle of Trust, https://www.digitaltrustcenter.nl/samenwerkingsverband/ciso-circle-of-trust
[77] Stichting NL CISO Circle of Trust ontvangt OKTT-status, https://www.banken.nl/nieuws/24811/stichting-nl-ciso-circle-of-trust-ontvangt-okktt-status
[78] Voor meer informatie over de CCoT zie ook de nota 'CISO Circle of Trust' aangedragen aan de Cyber Security Raad over verschillende strategische thema's aan het verkleinen van de cyberweerbaarheidskloof door middel van publiek-private samenwerking
[79] Landelijk Dekkend Stelsel, NCTV https://www.nctv.nl/onderwerpen/landelijk-dekkend-stelsel
[80] Landelijk Dekkend Stelsel, NCSC https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds
[81] DTC deelt informatie over cyberdreigingen met bedrijfsleven, https://www.digitaltrustcenter.nl/dreigingsinformatie-ontvangen

4.5 Observaties hulpmiddelen samenwerkingsverbanden

In deze sectie zijn observaties weergegeven die voort zijn gekomen uit het onderzoek naar de hulpmiddelen die worden aangeboden vanuit samenwerkingsverbanden. Het overzicht van de hulpmiddelen vanuit samenwerkingsverbanden kan vergeleken worden met het overzicht van de algemene hulpmiddelen.

In totaal worden er 187 hulpmiddelen aangeboden vanuit 51 samenwerkingsverbanden in Nederland (zie Tabel 12 in Appendix D – Overzicht samenwerkingsverbanden). Vanwege de grote hoeveelheid hulpmiddelen is er in het onderzoek gekozen om de hulpmiddelen eerst te clusteren aan de hand van de 'typen hulpmiddelen' en deze vervolgens te koppelen aan de obstakels; zie 4.2.2. Aanpak hulpmiddelen samenwerkingsverbanden' voor meer informatie. Het resultaat hiervan is te zien in Tabel 5.

		Type hulpmiddelen en aantallen aangeboden door samenwerkingsverbanden (gesorteerd op #)											
Obstakel (gesorteerd op #)		Schriftelijke kennisdeling en voorlichting	Bijeenkomst voor kennisdeling en bewustwording	Cybertools en -maatregelen, gratis of tegen gereduceerde prijs	Analyseren en delen van (acute) dreigingsinformatie voor handelingsperspectief	Professioneel advies en begeleiding	Voorlichtingscampagne	Certificaten en keurmerken	(Cyber) crisisoefening	Meldpunt en noodhulplijn	Database ICT leveranciers	Cyberverzekering	#
2B	Onvoldoende inzicht in handelingsperspectief	42		10	16	8				3			79
1	Onvoldoende cyberbewustzijn en –kennis	14	53	1			5						73
2A	Onvoldoende inzicht in risico's	5		8		1			4				18
3	Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden			6								1	7
6	Afhankelijkheidsrisico's in toeleveringsketen							4			2		6
5	Beperkte toepasbaarheid huidige cyberrichtlijnen voor het mkb	3		1									4
4	Algemeen tekort aan personeel met expertise in cyber en ICT												0
7	Beperkte vindbaarheid van (overheids)hulpmiddelen												0
8	Veranderend dreigingslandschap												0
	Totaal (#)	64	53	26	16	9	5	4	4	3	2	1	187

Tabel 5 Overzicht van het aantal hulpmiddelen aangeboden door samenwerkingsverbanden.

4.5.1 Vergelijking algemene hulpmiddelen en hulpmiddelen vanuit samenwerkingsverbanden

De overeenkomsten tussen het overzicht van de algemene hulpmiddelen en het overzicht van de hulpmiddelen vanuit de samenwerkingsverbanden zijn:

- De meeste hulpmiddelen zijn te koppelen aan het obstakel 'Onvoldoende inzicht in handelingsperspectief'.
- In verhouding worden er veel meer hulpmiddelen aangeboden die inzicht bieden in handelingsperspectief in vergelijking met hulpmiddelen die gericht zijn op het in kaart brengen van risico's. Ongeveer 15 keer zoveel voor de algemene hulpmiddelen en ongeveer vier keer zoveel voor de hulpmiddelen vanuit samenwerkingsverbanden.
- Er zijn geen hulpmiddelen gevonden die terug te koppelen zijn naar het obstakel 'Veranderend dreigingslandschap'.

De verschillen tussen het overzicht van de algemene hulpmiddelen en het overzicht van de hulpmiddelen vanuit de samenwerkingsverbanden zijn:

- Er worden meer hulpmiddelen aangeboden vanuit de samenwerkingsverbanden (187 totaal) in vergelijking met de algemene hulpmiddelen vanuit de overheid en private organisaties (64 totaal). Dit lijkt logisch gezien er veel meer private samenwerkingsverbanden zijn ten opzichte van overheidsinstanties. Twee belangrijke verschillen zijn wel dat niet elk samenwerkingsverband landelijk opereert terwijl de overheid dat wel doet, en dat de hulpmiddelen vanuit de overheid voor iedereen toegankelijk zijn. Dit is niet altijd het geval bij private partijen gezien voor bepaalde hulpmiddelen lidmaatschap vereist is, of de partij richt zich op een specifieke branche, regio of sector.
- Er zijn 73 hulpmiddelen vanuit de samenwerkingsverbanden die gericht zijn op het verhogen van cyberbewustzijn en kennis voor bedrijven binnen het mkb. Bij de algemene hulpmiddelen zijn er geen hulpmiddelen voor het verhogen van cyberbewustzijn en -kennis die specifiek gericht zijn op bedrijven binnen het mkb.

5. Stimuleren en verbeteren

5. Stimuleren en verbeteren

5.1 Introductie

Het doel van dit hoofdstuk is inzichtelijk maken hoe bedrijven binnen het mkb kunnen worden gestimuleerd om hun cyberweerbaarheid te verbeteren en een antwoord te geven op de vraag welke hulp nodig is om bedrijven binnen het mkb aan te zetten tot handelen. Dit hoofdstuk bouwt dan ook voort op de obstakels en hulpmiddelen die zijn geïdentificeerd in hoofdstukken 3 en 4.

Om deze vraag te beantwoorden worden drie perspectieven meegenomen die, in het geval van onderlinge samenhang, samengebracht worden. Deze perspectieven zijn:

- De aanbieder van hulp, ofwel publieke overheidsinstanties en private samenwerkingsverbanden die hulpmiddelen aanbieden aan bedrijven binnen het mkb ter versterking van hun cyberweerbaarheid.
- De ontvanger van hulp, in dit geval bedrijven binnen het mkb die hulpmiddelen van overheidsinstanties en samenwerkingsverbanden kunnen gebruiken.
- Het buitenland, waar gekeken wordt naar 'best practices' vanuit het Verenigd Koninkrijk, Frankrijk, Duitsland en Denemarken.

Om inzicht te krijgen in het huidige cyberweerbaarheidsniveau van elk bedrijf is tijdens de interviews met bedrijven binnen het mkb de CyberVeilig Check van het DTC doorlopen[82]. Deze informatie wordt in dit hoofdstuk gebruikt waar het van toegevoegde waarde kan zijn. Enkele variabelen die, op basis van de interviews, gemiddeld genomen duiden op een hoog cyberweerbaarheidsniveau zijn:

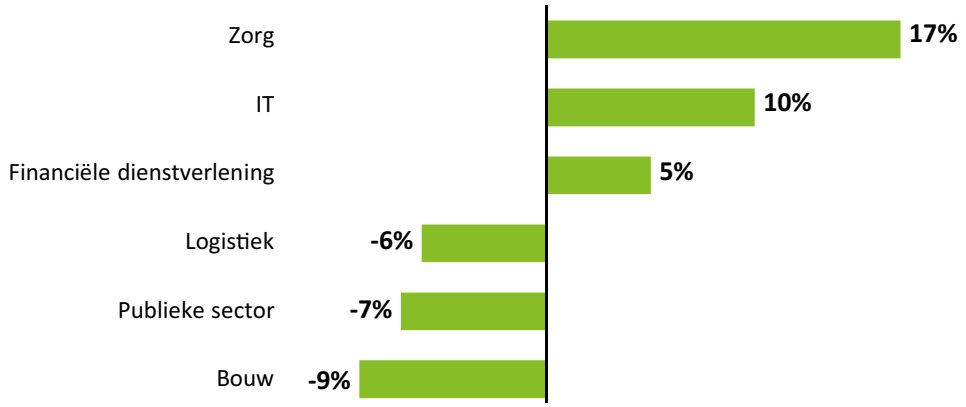
- De omvang van het bedrijf. Grotere bedrijven (in aantallen werknemers) hebben over het algemeen een hoger cyberweerbaarheidsniveau (zie Figuur 13 in Appendix F – Interviewdata), dit komt ook overeen met het 2023 deelrapport 'Cybersecurity onderzoek - bedrijfsleven' als onderdeel van Alert Online 2023[83].
- Het uitbesteden van ICT. Bedrijven met een hoger cyberweerbaarheidsniveau hebben vaak een ICT-dienstverlener (zie Figuur 13). Afgaande op de interviews kan de definitie van een ICT-leverancier wel variëren van een groter ICT-/ cyberveiligheidbedrijf waar vaste producten en diensten worden afgenomen, tot een zzp'er die geregeld ingehuurd wordt voor het oplossen van ICT-problemen.
- ICT inherent aan product/dienst. ICT-bedrijven hebben gemiddeld genomen een hoger cyberweerbaarheidsniveau omdat cyberveiligheid inherent is aan de producten en diensten die ze aanbieden (zie Figuur 13). Dit verklaart ook waarom bedrijven in de informatie- en communicatiesector gemiddeld genomen een hoger cyberweerbaarheidsniveau hebben (zie Figuur 6).
- ICT-functie binnen het bedrijf. Bedrijven met een hoger cyberweerbaarheidsniveau hebben vaker iemand in dienst die hier (deels) voor verantwoordelijk is (zie Figuur 13).
- Op maat gemaakte software. Bedrijven die naast SaaS (Software as a Service) ook op maat gemaakte software hebben, hebben vaker een hogere cyberweerbaarheid (zie Figuur 13).

Uit de interviews viel niet af te leiden wat de verschillen zijn tussen sectoren als het gaat om cyberweerbaarheid; hiervoor is aanvullend onderzoek nodig. Uit data van Eye Security[84] (zie Figuur 6) blijkt wel dat de sectoren Zorg, IT en Financiële dienstverlening gemiddeld een hogere cyberweerbaarheidsscore hebben. Logistiek, Publieke sector en de Bouw scoren daarentegen gemiddeld lager.

Figuur 6 bevat ruim 10.000 datapunten met minimaal 1.000 datapunten per sector. Deze datapunten zijn cyberweerbaarheidsscores van individuele bedrijven, waarbij het gemiddelde per sector wordt vergeleken met het gemiddelde van de gehele dataset van 10.000 datapunten. Elke cyberweerbaarheidsscore wordt gegenereerd op basis van 150 kenmerken waaraan een bedrijf voldoet. Eye Security heeft zelf deze lijst aan kenmerken vastgesteld. Dit gaat om geïmplementeerde technische beveiligingsmaatregelen, maar ook om maatregelen rond cyberbeleid en -bewustzijn. De bedrijven die zijn opgenomen in Figuur 6 hebben minimaal 15 werknemers. Het merendeel van de bedrijven heeft tot 200 medewerkers, enkele zitten boven de 250.

Cyberweerbaarheidsscore per sector ten opzichte van het gemiddelde

Klantdata van Eye Security



Figuur 6 Cyberweerbaarheidsscore per sector ten opzichte van het gemiddelde.

[82] Zie tools.digitaltrustcenter.nl, 'CyberVeilig Check voor ZZP en MKB'
[83] Zie rijksoverheid.nl, 'Deelrapport Cybersecurity onderzoek Alert Online 2023 – bedrijfsleven', 29 sep 2023
[84] Cyberbeveiligingsbedrijf dat onderdeel is van de klankbordgroep voor dit onderzoek

5.2 Aanpak

Om een beeld te krijgen van de drie perspectieven zijn er gesprekken gevoerd met de aanbieders van hulpmiddelen, bedrijven binnen het mkb en Deloitte experts uit het buitenland.

Er zijn in totaal 49 gesprekken gevoerd (47 interviews en 2 schriftelijk), waarvan 32 interviews met bedrijven binnen het mkb, 10 interviews met aanbieders van hulpmiddelen (2 aanbieders hebben schriftelijk informatie gedeeld), 4 interviews met Deloitte experts uit het buitenland en 1 interview met een gemeente.

- **32 interviews met bedrijven binnen het mkb.** Om de anonimiteit van de bedrijven binnen het mkb te waarborgen, worden er geen bedrijfsnamen genoemd. Voor een overzicht van het type bedrijven zie Tabel 1.
- **10 interviews met aanbieders van hulpmiddelen.** Voor de volledige lijst, zie Tabel 13. Deze lijst bestaat uit publieke partijen (DTC, EZK, VWS, Nationale Politie) en private partijen (CIP, Eye Security, ING, NLdigital, HSD, VNG). Naast de 10 interviews hebben het NCSC en de KVK schriftelijk informatie gedeeld. Voor de evaluatie van hulpmiddelen (zie 5.4.7 Obstakel 7: Beperkte vindbaarheid van (overheids-) hulpmiddelen) zijn alleen het DTC, NCSC, KVK en VWS benaderd met de vraag of ze data konden aanleveren over de effectiviteit van de hulpmiddelen die ze aanbieden. Deze vier partijen zijn gekozen vanwege de hulpmiddelen die ze aanbieden (zie Tabel 4) en hun rol in het verkleinen van de cyberweerbaarheidskloof[85].
- **4 interviews met Deloitte experts uit het buitenland.** Er zijn 4 interviews gehouden met Deloitte experts uit het buitenland. Deze gesprekken zijn gevoerd om een beeld te krijgen van de overheidsinitiatieven op het gebied van cyberweerbaarheid binnen het mkb in het Verenigd Koninkrijk, Frankrijk, Duitsland en Denemarken. Het doel is om inzichtelijk te maken in hoeverre we kunnen leren van andere landen. Er is een inventarisatie gemaakt van de overheidsinitiatieven in het buitenland[86]; bij een aantal oplossingsrichtingen zijn deze als voorbeeld toegevoegd. Hierbij is de werking van de buitenlandse overheidsinitiatieven niet getoetst. In hoeverre deze buitenlandse overheidsinitiatieven ook werken binnen de Nederlandse context vereist vervolgonderzoek.
- **1 interview met een gemeente.** Gemeenten ervaren vaak vergelijkbare problemen in het versterken van hun eigen cyberweerbaarheid ten opzichte van bedrijven binnen het mkb. Gezien gemeenten niet binnen het mkb vallen wordt deze apart genoemd.

Alle informatie uit de interviews is geanalyseerd om kwantitatieve en kwalitatieve inzichten te verkrijgen met betrekking tot de obstakels, hulpmiddelen, behoeftes en rol van de overheid.

- **Data-analyse van de interviews met bedrijven binnen het mkb.** Een kwantitatieve analyse van de data van de interviews met bedrijven binnen het mkb dient alleen ter ondersteuning van kwalitatieve bevindingen van de interviews. De dataset is namelijk te klein om een volledig kwantitatief onderzoek uit te voeren.
- **Data-analyse van de interviews met aanbieders en Deloitte experts.** Alleen kwalitatieve inzichten zijn verkregen op basis van de interviews met de aanbieders en Deloitte experts.

5.3 Mogelijkheden die leiden tot verbetering

Om de mogelijkheden die leiden tot verbetering te kunnen identificeren is er een koppeling gemaakt tussen de obstakels, het huidige aanbod van de hulpmiddelen en de behoefte van bedrijven binnen het mkb. Vervolgens is in kaart gebracht in hoeverre het aanbod van hulpmiddelen aansluit bij de behoefte van het mkb. Deze informatie staat beschreven in Tabel 6. Verder is er ook voor zover mogelijk gekeken naar het gebruik en de effectiviteit van de hulpmiddelen (zie 5.4.7 Obstakel 7: Beperkte vindbaarheid van (overheids-) hulpmiddelen).

[85] VWS is uiteindelijk niet meegenomen in de evaluatie in 5.4.7 gezien het hulpmiddel OpenKAT niet relevant is voor bedrijven binnen het mkb omdat het een relatief hoog kennis-niveau vereist

[86] Zie appendix I voor het volledige overzicht

		Obstakel	Obstakels	Hulpmiddelen		Behoefte vanuit interviews met bedrijven binnen het mkb	Behoefte	Hulp sluit aan bij behoefte
			# (%)	Publiek #	Privaat #		# (%)	
Intern	1	Onvoldoende cyberbewustzijn en –kennis	27 (84%)	2	2	Verbinding, communicatie en voorlichting	22 (69%)	🔴
Intern	2	Onvoldoende inzicht in risico's	16 (50%)	2	2	Handelingsperspectief dat aansluit op risicoprofiel	15 (47%)	🟠
Intern	2	Onvoldoende inzicht in handelingsperspectief	9 (28%)	28	17			
Intern	3	Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden	19 (59%)	3	-	Financiële ondersteuning	9 (28%)	🟡
Extern	4	Algemeen tekort aan personeel in Nederland met expertise in ICT en cyberveiligheid	3 (9%)	-	1	*Nvt*	-	⚪
Extern	5	Beperkte toepasbaarheid huidige cyberrichtlijnen voor het mkb	2 (6%)	2	-	Duidelijke regels en handhaving	7 (22%)	🟡
Extern	6	Afhankelijkheidsrisico's in toeleveringsketen	2 (6%)	1	3	Selectie van en samenwerking met ICT leveranciers	10 (31%)	🔴
						Certificering	5 (16%)	🟠
Extern	7	Beperkte vindbaarheid van (overheids-)hulpmiddelen	3 (9%)	1	-	Wegwijzer cyberveiligheid	4 (13%)	🟠
						Centraal punt met hulplijn	3 (9%)	🟠
Extern	8	Veranderend dreigingslandschap	1 (3%)	-	-	*Nvt*	-	⚪

🟡 Grotendeels 🟠 Deels 🔴 Onvoldoende aandacht voor behoefte

Tabel 6 Duiding in hoeverre de hulp die aangeboden wordt, aansluit bij de behoefte van bedrijven binnen het mkb. Voor de data in kolommen 'Obstakels' en 'Behoefte' zie Appendix F. De percentages laten zien welk deel van de in totaal 32 geïnterviewden aan hebben gegeven dat een bepaald obstakel of behoefte voor hen van toepassing is. De kleurcodering geeft aan in hoeverre de hulp aansluit bij de behoefte, en is gebaseerd op een kwalitatieve analyse van de aangeboden hulpmiddelen en de uitgesproken behoeftes van de mkb'ers.

5.4 Onderbouwing mogelijkheden die leiden tot verbetering

In dit hoofdstuk wordt er per obstakel beschreven wat het huidig aanbod van de hulpmiddelen is, wat de uitdagingen zijn met betrekking tot het aanbod van de hulpmiddelen zijn en wat een mogelijke oplossing is op basis van de behoefte van het mkb.

5.4.1 Obstakel 1: Onvoldoende cyberbewustzijn en -kennis

Het huidige aanbod van de hulpmiddelen

Voor het obstakel 'Onvoldoende cyberbewustzijn en -kennis' worden er 4 hulpmiddelen aangeboden vanuit de overheid en private organisaties (zie Tabel 4). Dit zijn vrij omvattende hulpmiddelen zoals bijvoorbeeld het 'Overheidsbreed Cyberprogramma (BZK)'. Daarnaast wordt er wel veel kennis gedeeld ter bevordering van het cyberbewustzijn via samenwerkingsverbanden (73 in totaal, zie Tabel 5).

Uitdagingen met betrekking tot het aanbod van de hulpmiddelen

De hulpmiddelen die worden aangeboden vanuit de overheid kunnen breed toegepast worden en zijn niet specifiek toegespitst op bedrijven binnen het mkb, bepaalde sectoren of het type bedrijf. Geïnterviewden geven aan niet of slechts beperkt bekend te zijn met hulpmiddelen die aangeboden worden vanuit de overheid voor het verhogen van hun cyberbewustzijn en kennis. Enkel 9% geeft bijvoorbeeld aan bekend te zijn met het DTC (zie Figuur 11). Uit onderzoek van het DTC in 2023 blijkt dat 20% van de bedrijven bekend is met het DTC[87]. Geïnterviewden geven aan dat ze vooral worden aangezet tot handelen doordat ze in het nieuws en om zich heen zien wat de impact kan zijn van een cyberincident (zie Figuur 9).

Hierop voortbouwend lijkt de grotere uitdaging dat het belang van het obstakel 'Onvoldoende cyberbewustzijn en -kennis' wordt onderschat door de aanbieders van hulpmiddelen. 84% van de geïnterviewden geeft aan dat dit voor hen een belangrijk obstakel is (zie Figuur 10), en noemen dit obstakel ook vaak in combinatie met obstakels 2 en 3, wat duidt op het feit dat bewustzijn en kennis fundamenteel zijn (zie Tabel 14). Geïnterviewden geven aan dat een onderliggende oorzaak van onvoldoende bewustzijn en -kennis ook kan komen doordat ze te weinig tijd en capaciteit hebben voor het versterken van cyberweerbaarheid. Dit komt uiteindelijk neer op de prioritering van werkzaamheden, wat op zichzelf kan betekenen dat het cyberbewustzijnsniveau te laag is. Een andere onderliggende oorzaak die geïnterviewden deelden is

[87] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023

dat de informatie die de overheid verstrekt in hun ogen niet altijd effectief is. Zij geven aan dat de informatie vaak gericht is op de samenleving in het algemeen of gefocust is op grotere bedrijven waardoor het minder toepasbaar is voor bedrijven binnen het mkb.

> ***"Als zzp'er heb je naast je klantwerk nog veel andere dingen waar je mee bezig bent. Cybersecurity staat onderaan de prioriteitenlijst. Er is geen bewustzijn en kennis van het belang of de noodzaak van cyber omdat niet duidelijk is wat het risico is voor het bedrijf."***
> Quote van geïnterviewde mkb'er

Oplossing op basis van de behoeftes van het mkb
69% van de geïnterviewde bedrijven binnen het mkb (zie Tabel 15) heeft behoefte aan:

1. **Bewustzijn creëren van de urgentie van cybersecurity.** Een eerste stap in het versterken van de cyberweerbaarheid van het mkb is dat er bewustzijn moet ontstaan over het belang en de urgentie van cybersecurity. Zonder dit bewustzijn zullen bedrijven binnen het mkb überhaupt geen stappen nemen om te verbeteren of de overheid benaderen voor hulpmiddelen. Uit de interviews blijkt dat angst voor omzetverlies (34%), het nieuws (31%), zelf gehackt zijn (25%), angst voor reputatieschade (25%) en vragen vanuit klanten (22%) de belangrijkste aanleidingen zijn voor het mkb om hun cyberweerbaarheid te gaan versterken (zie Figuur 9). Bewustzijnscampagnes vanuit de overheid kunnen gericht worden op deze onderwerpen om urgentie te creëren bij het mkb. Daarnaast dient cyberveiligheid ook zo te worden gepositioneerd dat het in positieve zin juist kan bijdragen aan het vertrouwen van klanten en leveranciers. Op deze manier is cyberveiligheid niet alleen een risico dat afgedekt moet worden, maar ook een kans om onderscheidend te zijn.
2. **Relevante partijen verbinden.** Er dient een sterkere verbinding te zijn met relevante partijen om in gesprek te gaan en samen te werken aan cyberweerbaarheid van het mkb. Horizontaal gaat dit om verbinding met (lokale) mede-mkb'ers en dienstverleners, en verticaal gaat dit om de verbinding met brancheverenigingen, gemeente/provincie en de Rijksoverheid. De partijen die hulpmiddelen maken moeten hun krachten bundelen en ook zorgen voor een goede onderlinge (inhoudelijke) afstemming. Op die manier kan een evenwichtig aanbod worden samengesteld dat op alle terreinen hulpmiddelen biedt.
   Samenwerkingsverbanden spelen hier een belangrijke rol. Dit is geen nieuwe oplossing; het DTC is sinds haar oprichting in 2018 actief bezig met het subsidiëren en ondersteunen van samenwerkingsverbanden tussen bedrijven[88]; inmiddels zijn het er 58[89]. Een van deze samenwerkingsverbanden is het Cyber Weerbaarheidscentrum Greenport[90], opgezet in samenwerking met onder andere The Hague Security Delta (HSD). CW Greenport is een organisatie zonder winstoogmerk, waarbij verschillende bedrijven uit de tuinbouwindustrie samenwerken om zelf maar juist ook als industrie cyberweerbaar te zijn.
3. **Concrete, toegankelijke en doelgerichte communicatie in de omgeving van het bedrijf.** Er is behoefte aan concrete, toegankelijke en doelgerichte communicatie, tussen de aanbieders van hulpmiddelen en bedrijven binnen het mkb. Belangrijk is dat de communicatie verloopt via betrouwbare kanalen waar bedrijven binnen het mkb bekend mee zijn, of bekend mee kunnen worden omdat ze er niet omheen kunnen; voorbeelden zijn de KVK of de accountant waar ze toch al vaste contactmomenten mee hebben. Verder is er behoefte aan meer directe communicatie, zoals bijvoorbeeld via de post of mail, en aan een waarschuwingssysteem voor het delen van dreigingsinformatie.
4. **Training en voorlichting geven.** Een belangrijk doel van deze communicatie is training en voorlichting geven, waarbij informatie, inzichten, kennis en kunde gedeeld worden en leiden tot inzicht in risico's en handelingsperspectief. Uit onderzoek van het DTC in 2023, blijkt dat 42% van de bedrijven hun personeel vrijwillige training omtrent ICT-veiligheid liet volgen, dat 27% van de bedrijven in 2023 hun personeel verplichte training omtrent ICT-veiligheid liet volgen en 36% van de bedrijven training met contract aanbood[91].

Een voorbeeld is het 'Alliance for Cyber Security' samenwerkingsplatform uit Duitsland[92]. Dit platform is in 2012 opgericht en biedt bedrijven, verenigingen, autoriteiten en organisaties een manier waarop informatie over actuele dreigingssituaties en praktische maatregelen op het gebied van cyberbeveiliging uitgewisseld kunnen worden. Deelnemers profiteren van de kennis van de betrokken partners en kunnen daardoor de bescherming van hun eigen IT-infrastructuur aanzienlijk verbeteren.

5.4.2 Obstakel 2: Onvoldoende inzicht in risico's en handelingsperspectief

Het huidige aanbod van de hulpmiddelen
Voor het obstakel 'Onvoldoende inzicht in risico's' worden 4 hulpmiddelen aangeboden vanuit de overheid en private organisaties (zie Tabel 4). Vanuit de overheid is dit bijvoorbeeld de Risicoklasse Tool van het DTC. Vanuit de samenwerkingsverbanden worden er 19 hulpmiddelen aangeboden voor het verkrijgen van inzicht in risico's (zie Tabel 5).

Voor het obstakel 'Onvoldoende inzicht in handelingsperspectief' worden 45 hulpmiddelen aangeboden vanuit de overheid en private organisaties (zie Tabel 4). Vanuit de samenwerkingsverbanden worden er 79 hulpmiddelen aangeboden voor het verkrijgen van inzicht in handelingsperspectief (zie Tabel 5).

88 Zie DTC.nl, 'Subsidieregeling Cyberweerbaarheid stimuleert samenwerkingsverbanden'
89 Zie DTC.nl, 'Overzicht van samenwerkingsverbanden'; de website vermeldt dat er 54/56 samenwerkingsverbanden zijn, echter bevat de volledige lijst zonder dubbelingen 58 samenwerkingsverbanden
90 Zie cwgreenport.nl
91 Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
92 Zie bsi.bund.de, 'Alliance for Cyber Security'

Uitdagingen met betrekking tot het aanbod van de hulpmiddelen
Hoewel er beduidend minder hulpmiddelen zijn voor het creëren van inzicht in risico's versus handelingsperspectief (zie Figuur 5), lijkt het probleem niet te zijn dat er te weinig hulp geboden wordt. De uitdaging ligt in de samenhang en diepgang van de hulp. De hulpmiddelen die worden aangeboden vanuit de overheid geven namelijk geen grondige en onderbouwde analyse van de risico's, en koppelen deze niet direct aan maatregelen die specifiek van toepassing zijn op een individueel bedrijf. Hierdoor blijft het lastig voor bedrijven binnen het mkb om te bepalen wat hun grootste risico's zijn, en hoe ze daar mee om moeten gaan. Geïnterviewden onderstrepen het belang van dit obstakel in zijn geheel, waarbij opvalt dat de nadruk ligt op het creëren van inzicht in risico's, terwijl de hulpmiddelen in aantallen meer gericht zijn op handelingsperspectief (zie Tabel 4).

Ondanks dat het type hulp niet volledig aansluit op de behoefte, geeft 44% van de geïnterviewden aan toch risicoanalyses te hebben uitgevoerd (zie Figuur 11). Dit kan verschillen van een werkstudent die als onderdeel van het afstudeerproject gekeken heeft naar zwakke punten van het bedrijf, tot risicoanalyses als onderdeel van de ISO27001 certificering. Uit onderzoek van het DTC in 2023, blijkt dat 55% van de bedrijven risicoanalyses uitvoert[93]

Geïnterviewden geven aan dat als een bedrijf geen risicoanalyse uitvoert, de onderliggende oorzaak is dat bedrijven "naïef zijn en denken geen target te zijn". Dit geeft aan dat obstakel 2 een duidelijke verbinding heeft met obstakel 1 'Het gebrek aan cyberbewustzijn en kennis'. Deze worden dan ook vaak samen genoemd (zie Tabel 14).

Er worden veel hulpmiddelen aangeboden vanuit de overheid voor het verkrijgen van inzicht in handelingsperspectief[94]. Hierdoor ontstaat het risico dat er zo'n groot aanbod is van verschillende partijen, dat de bedrijven binnen het mkb niet meer kunnen valideren wat voor hen van belang is. Het ruime aanbod aan hulpmiddelen vanuit verschillende publieke organisaties (DTC, KVK, NCSC, RVO, Autoriteit Persoonsgegevens, RDI, Digitale Overheid) kan dus verlammend werken omdat het niet duidelijk is wat wel of niet van toepassing en/of belangrijk is.

Oplossing op basis van de behoeftes van het mkb
Uit de interviews blijkt dat mkb'ers behoefte hebben aan concreet handelingsperspectief dat is gebaseerd op het risicoprofiel van het bedrijf. Dit heeft als doel bedrijven binnen het mkb te helpen met de afweging tussen veiligheid en de benodigde investeringen, ofwel, "wanneer is goed, goed genoeg?". Dit hulpmiddel bevat idealiter de volgende informatie:

1. **Eenduidige basismaatregelen bieden.** Deze basismaatregelen zouden moeten gelden voor elk bedrijf binnen het mkb. Dit is het laaghangend fruit: cyberweerbaarheidsmaatregelen die gratis of goedkoop zijn, makkelijk te implementeren en onafhankelijk van het type bedrijf of het risicoprofiel. Denk bijvoorbeeld aan het maken van een back-up van de belangrijkste bedrijfsgegevens. Er is nu keuze uit verschillende maatregelen; stel er een aantal centraal[95].
2. **Inzicht bieden in de risico's van een bedrijf.** Deze analyse dient ook te beschrijven in hoeverre deze risico's zijn afgedekt. De overheid zou dit verplicht kunnen stellen, waarbij een bedrijf bijvoorbeeld elk jaar een vragenlijst in moet vullen om aan te geven welke risico's het bedrijf loopt en welke maatregelen geïmplementeerd zijn. Dit zou ook via de accountant kunnen, die verplicht wordt te vragen naar de cyberweerbaarheid van het bedrijf bij het opstellen van het jaarverslag. Belangrijk hier is wel dat de risicoanalyse volledig is en tot op een bepaald niveau maatwerk is.
3. **Additionele maatregelen vaststellen.** Additionele maatregelen die geïmplementeerd moeten/kunnen worden op basis van het type bedrijf en het risicoprofiel. Deze additionele maatregelen kunnen eventueel ingedeeld worden in verschillende ambitieniveaus, zoals 'basis+', 'gevorderd' en 'professioneel'. Eventueel kan ook aangegeven worden in hoeverre maatregelen wettelijk verplicht zijn, zoals maatregelen rondom de privacy van persoonsgegevens.

Er zijn veel hulpmiddelen die de informatie van de hiervoor genoemde punten (deels) bevatten. Het moet met name nog gebundeld worden, en gekoppeld worden aan een uitgebreidere risicoanalyse. 47% van de geïnterviewden zou geholpen zijn met een gratis, online tool die dit inzicht in risico's en handelingsperspectief aanbiedt (zie Figuur 12).

Deze oplossing dekt ook voor een deel obstakel 3 af waar het probleem is dat bedrijven niet weten hoeveel en waarin geïnvesteerd moet worden. Verder is ook de koppeling te maken met obstakel 6 'Afhankelijkheidsrisico's in de toeleveringsketen'. De tool zoals hierboven beschreven zou ook gekoppeld kunnen worden aan een database met ICT-leveranciers, zodat de juiste ICT-leverancier gekozen kan worden op basis van de benodigde cyberweerbaarheidsmaatregelen. Een dergelijke database is al beschikbaar in het Verenigd Koninkrijk[96], Frankrijk[97] en Denemarken (D-seal)[98].

"Er is een gebrek aan inzicht; er zijn heel veel aanbieders van IT en cyber die verschillende producten en diensten aanbieden waardoor het niet duidelijk is wat de juiste kosten/baten balans is. Het grootste obstakel is het ontbreken van kennis en bij welke IT-dienstverlener je nou moet beginnen."
Quote van geïnterviewde mkb'er

93 Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
94 Op basis van de interviews is niet te achterhalen welke van deze hulpmiddelen het meest worden gebruikt of het beste werken
95 Welke maatregelen specifiek meegenomen dienen te worden zal duidelijk moeten worden uit een vervolgonderzoek
96 Zie ncsc.gov.uk, 'Verify suppliers'
97 Zie cybermalveillance.gouv.fr, 'The professionals listed'
98 Zie d-seal.eu

5.4.3 Obstakel 3: Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden

Het huidige aanbod van de hulpmiddelen
Voor het obstakel 'Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden', worden er drie hulpmiddelen aangeboden vanuit de overheid: twee subsidieregelingen en een meer overkoepelend hulpmiddel, namelijk sancties voor het overtreden van privacywetgeving (zie Tabel 4). Subsidies zijn een positieve financiële prikkel en sancties kunnen gedefinieerd worden als een negatieve financiële prikkel. Daarnaast worden er 7 hulpmiddelen aangeboden via samenwerkingsverbanden (zie Tabel 5).

Uitdagingen met betrekking tot het aanbod van de hulpmiddelen
Afgaande op het aanbod aan hulpmiddelen, lijkt de overheid voor dit obstakel zich vooral te richten op het aanbieden van financiële middelen en handhaving van wet- en regelgeving. Beiden zijn belangrijk en sluiten (deels) aan bij de behoefte van de geïnterviewden, maar er mist inzicht in hoeveel en waarin geïnvesteerd moet worden door bedrijven binnen het mkb. Dit punt raakt aan het gebrek aan handelingsperspectief en de genoemde oplossing in 5.4.2 Obstakel 2: Onvoldoende inzicht in risico's en handelingsperspectief'. Geïnterviewden geven namelijk aan moeite te hebben met het vinden van de juiste 'kosten-batenbalans'. Hoeveel moet je investeren om veilig genoeg te zijn, en hoe rendabel zijn die investeringen?

> ***"Het is moeilijk om in te schatten hoeveel tijd en geld je moet investeren om voor jouw bedrijf voldoende cyberweerbaar te zijn."***
> Quote van geïnterviewde mkb'er

Geïnterviewden geven wel duidelijk aan dat het versterken van hun cyberweerbaarheid hun eigen verantwoordelijkheid is, en dat ze bereid zijn hierin te investeren zolang ze weten waarin ze investeren, en in hoeverre het de risico's afdekt. Het anticiperen op risico's en het investeren in kansen is simpelweg onderdeel van het ondernemerschap, ook als het gaat om cyberveiligheid.

> ***"Het mkb moet zijn eigen broek ophouden, en als het fout gaat, gaat het fout."***
> Quote van geïnterviewde mkb'er

Los van niet weten waarin te moeten investeren, geven sommige bedrijven ook aan dat er een tekort is aan financiële middelen, waarna de bewuste keuze werd gemaakt bepaalde cyberveiligheidsmaatregelen niet te implementeren vanwege de hoge kosten; denk bijvoorbeeld aan een penetratietest, een cyberverzekering en een onderzoek naar een cyberincident. Deze behoefte aan financiële ondersteuning is ook terug te zien in het feit dat de subsidieregeling 'Mijn Cyberweerbare Zaak' na drie weken al overtekend was[99].

Het ontbreken van financiële middelen is overigens niet voor iedereen een probleem. De twee bedrijven die 'Nee' hebben geantwoord op de vraag of obstakel 3 een probleem is (zie Figuur 10), hebben een voldoende tot goed cyberweerbaarheidsniveau vergeleken met de rest.

Oplossing op basis van de behoeftes van het mkb
Uit de interviews blijkt dat bedrijven binnen het mkb, aangaande dit obstakel, behoefte hebben aan het volgende:

1. **Subsidies aanbieden.** Het aanbieden van subsidies voor cyberweerbaarheid en ondersteuning bieden bij het aanvragen van subsidies; dit moet simpel en snel zijn gezien geïnterviewden vaak aangeven weinig tijd te hebben en kennis/ervaring te missen over het invullen van subsidieaanvragen.
2. **Gratis (of tegen een gereduceerd tarief) maatregelen aanbieden.** Sommige geïnterviewden geven aan dat de financiële ondersteuning vanuit de overheid gericht moet zijn op het aanbieden van gratis (of tegen een gereduceerd tarief) preventieve maatregelen. Bijvoorbeeld dat er vouchers voor penetratietesten beschikbaar worden gesteld waarbij de overheid een deel van de kosten dekt.

De overheid dient te helpen met het maken van een inschatting van de benodigde investeringen voor het implementeren van cyberweerbaarheidsmaatregelen. Daarnaast, indien mogelijk, dient ook inzicht gegeven te worden in wat de maatregelen opleveren door bijvoorbeeld aan te geven wat de financiële schade kan zijn van een cyberincident, dat voorkomen kan worden door een specifieke maatregel.

Het is niet duidelijk wat 'best practices' zijn op dit gebied vanuit het buitenland.

5.4.4 Obstakel 4: Algemeen tekort aan personeel met expertise in ICT en cyberveiligheid

Het huidige aanbod van de hulpmiddelen
Voor het obstakel 'Algemeen tekort aan personeel in Nederland met expertise in ICT en cyberveiligheid' wordt er één hulpmiddel aangeboden vanuit een private partij (Security Delta, zie Tabel 4). Daarnaast worden er geen hulpmiddelen aangeboden via samenwerkingsverbanden (zie Tabel 5).

[99] 'DTC introduceert cybersubsidie voor kleine bedrijven', DTC, 27 oktober 2023

Uitdagingen met betrekking tot het aanbod van de hulpmiddelen
Vanuit de overheid zijn er geen hulpmiddelen gevonden die direct dit probleem helpen oplossen voor bedrijven binnen het mkb. De overheid lijkt meer gericht op langetermijnoplossingen door bijvoorbeeld ICT en cyberveiligheid onderdeel te maken van het onderwijs. Op dit vlak zijn publieke en private partijen actief waarbij vooruitgang boeken uitdagend kan zijn[100], hoewel uit de verkiezingsprogramma's van 2023 blijkt dat bijna alle partijen aandacht schenken aan digitale geletterdheid in het primair onderwijs[101]. Een belangrijk initiatief is Curriculum.nu waar onder andere nieuwe kerndoelen ontwikkeld zijn op negen leergebieden, waaronder Digitale Geletterdheid[102]. In navolging hierop is Stichting Leerplan Ontwikkeling (SLO) gevraagd door het Ministerie van Onderwijs, Cultuur en Wetenschap om conceptkerndoelen op te stellen voor eind 2023. Ook wordt in het najaar van 2023 een 'Expertisepunt digitale geletterdheid' ingericht door SLO om relevante informatie over beleid en praktijk te verzamelen en te delen .

Het obstakel 4, 'Algemeen tekort aan personeel in Nederland met expertise in ICT en cyberveiligheid', wordt maar door 9% van de geïnterviewden genoemd (zie Figuur 10). Een mogelijke oorzaak hiervoor is dat bedrijven binnen het mkb weinig invloed hebben op dit bredere maatschappelijke probleem, en dus meer focussen op interne obstakels zoals cyberbewustzijn en -kennis of handelingsperspectief. Vanuit de interviews geven met name kleinere bedrijven aan de capaciteit niet te hebben om personeel aan te nemen met specifieke ICT/cyberkennis. Als je als bedrijf binnen het mkb toch meer wilt doen met cyberveiligheid, dan is het aannemen van een expert op dit gebied waarschijnlijk niet de eerste oplossing.

Oplossing op basis van de behoeftes van het mkb
Op basis van de interviews is er niet een expliciete behoefte naar voren gekomen voor het aanbieden van hulpmiddelen voor het oplossen van het tekort aan personeel met kennis van ICT en cyberveiligheid. Voor een kortetermijnoplossing voor het tekort aan personeel lijkt een bedrijf binnen het mkb vooralsnog aangewezen op zichzelf, samenwerkingsverbanden of het (individueel of gezamenlijk) inhuren van commerciële partijen.

5.4.5 Obstakel 5: Beperkte toepasbaarheid huidige cyber-richtlijnen voor het mkb

Het huidige aanbod van de hulpmiddelen
Voor het obstakel 'Beperkte toepasbaarheid huidige cyberrichtlijnen voor het mkb' worden er twee hulpmiddelen aangeboden vanuit de overheid (zie Tabel 4). Dit zijn online informatiepagina's die betrekking hebben op AVG en NIS2. Daarnaast worden er vier hulpmiddelen aangeboden via samenwerkingsverbanden (zie Tabel 5). Een voorbeeld hiervan is de webpagina 'De NIS2 wet' van Samen Digitaal Veilig (zie Tabel 4).

Uitdagingen met betrekking tot het aanbod van de hulpmiddelen
Hoewel er hulpmiddelen zijn die wet- en regelgeving rondom cyberveiligheid vertalen naar begrijpelijke richtlijnen, lijkt de toepasbaarheid op het mkb onvoldoende, zeker als het gaat om toepasbaarheid binnen een specifieke sector. Met andere woorden: de hulpmiddelen lijken algemeen toepasbaar voor een breed publiek, waarbij er een vertaling mist van de richtlijnen naar bijvoorbeeld een specifieke sector.

In 2 interviews en in de klankbordgroep kwam naar voren dat sommige mkb'ers "hun kop in het zand steken totdat ze op de vingers worden getikt" en "niet het beste jongetje van de klas hoeven te zijn". Voldoen aan wet- en regelgeving rondom cyberveiligheid lijkt niet altijd een prioriteit te zijn.

Oplossing op basis van de behoeftes van het mkb
Vanuit de interviews geven bedrijven binnen het mkb aan dat de overheid wel kaders schetst voor de cyberveiligheid van bedrijven, maar bedrijven vervolgens vrij laat om dit zelf in te vullen[104].

> ***"Er is niks wat jou verplicht om iets te doen met cybersecurity, en als het er al is, is het niet bekend bij de gemiddelde mkb'er; er is duidelijkheid nodig, inclusief handvatten vanuit de overheid over waar je aan moet voldoen op basis van het type bedrijf."***
> Quote van geïnterviewde mkb'er

Er zijn goede voorbeelden van richtlijnen zoals 'Stappenplan: AVG op orde voor ondernemers en mkb' van de Autoriteit Persoonsgegevens[105]. Er is behoefte aan meer van dit soort hulpmiddelen, zeker als het gaat om NIS2, gezien bedrijven verplicht worden om cybermaatregelen te gaan implementeren. In het Verenigd Koninkrijk biedt het NCSC dit soort hulpmiddelen aan, waarbij de vertaling van wetgeving naar richtlijnen aangepast wordt per industrie[106]. Naast duidelijke wet- en regelgeving dient de overheid dus ook ondersteuning aan te bieden in het naleven ervan, en dient er duidelijke toezicht en handhaving te zijn zodat bedrijven binnen het mkb weten waar ze aan toe zijn en middels de juiste maatregelen geactiveerd worden om stappen te ondernemen in het versterken van hun cyberweerbaarheid.

> ***"De overheid moet duidelijk maken waar je aan moet voldoen [als het gaat om cyberweerbaarheid], net als bij een APK."***
> Quote van geïnterviewde mkb'er

[100] NLdigital: 'Tweede Kamer dreigt digitale geletterdheid alsnog weg te bezuinigen', 26 mei 2023
[101] NLdigital: 'Nieuwkomers BBB en Volt hebben sterkste programma op gebied van digitalisering', 9 nov 2023
[102] Zie Curriculum.nu
[103] Kennisnet.nl: 'Expertisepunt digitale geletterdheid in het najaar gelanceerd', 25 september 2023
[104] Hoewel geen van de geïnterviewde bedrijven binnen het mkb aangaf bekend te zijn met NIS2, zal deze wetgeving de regels voor bedrijven die eronder vallen wel degelijk aanscherpen
[105] Zie www.autoriteitpersoonsgegevens.nl 'AVG voor ondernemers'
[106] Zie ncsc.gov.uk, 'Small & medium sized organisations – Support for sectors'

5.4.6 Obstakel 6: Afhankelijkheidsrisico's in de toeleveringsketen

Het huidige aanbod van de hulpmiddelen
Voor obstakel 6, 'Afhankelijkheidsrisico's in de toeleveringsketen', is er één hulpmiddel gevonden vanuit de overheid: 'Afspraken maken met een IT-leverancier' van het DTC. Er zijn verder verschillende commerciële partijen die online tips geven over welke vragen je moet stellen aan je ICT-dienstverlener; deze worden buiten beschouwing gelaten. Er worden verder drie hulpmiddelen aangeboden vanuit private partijen (zie Tabel 4), waaronder de CYRA Cyber Rating, het groot-helpt-klein principe (zie bijvoorbeeld het initiatief CISO Circle of Trust van ASML) en het keurmerk voor ICT-dienstverleners van de CCV (nog in ontwikkeling). Daarnaast worden er zes hulpmiddelen aangeboden via samenwerkingsverbanden (zie Tabel 5).

Uitdagingen met betrekking tot het aanbod van de hulpmiddelen
Dit obstakel wordt door 6% van de geïnterviewden genoemd (zie Figuur 10); dit is een stuk minder dan de interne obstakels. Deze twee bedrijven hebben een gemiddeld en goed cyberweerbaarheidsniveau, dit kan de reden zijn dat ze meer bewust zijn van de afhankelijkheidsrisico's in de toeleveringsketen.

31% van de bedrijven (zie Figuur 12) hebben echter wel de behoefte geuit voor hulp bij het selecteren en samenwerken met ICT-leveranciers, en 16% van de bedrijven hebben behoefte aan een certificering voor ICT-leveranciers (zie Figuur 12). Deze behoeftes zijn gekoppeld aan dit obstakel, gezien de ICT-leverancier onderdeel is van de toeleveringsketen van het bedrijf binnen het mkb. Een verklaring voor het feit dat enkel 2 geïnterviewden dit als een obstakel noemen, kan zijn omdat het merendeel het samenwerken met een ICT-leverancier niet als afhankelijkheidsrisico zien, maar enkel als een oplossing voor hun problemen omtrent cyberveiligheid.

> ***"De SLA met de IT-dienstverlener is slecht uitgewerkt waardoor het onduidelijk is wat de onderlinge verwachtingen zijn."***
> Quote van geïnterviewde mkb'er

Zoals weergegeven in Tabel 6, sluit de hulp voor het selecteren van en omgaan met ICT-leveranciers deels aan op de behoeftes van bedrijven binnen het mkb. De behoefte om hulp bij de omgang met ICT-leveranciers wordt deels afgedekt door het hulpmiddel vanuit het DTC; over de effectiviteit van dit hulpmiddel is geen informatie beschikbaar vanuit het DTC. Voor het selecteren van de juiste ICT-leverancier is weinig aandacht, hoewel dit nu wel in ontwikkeling is door het CCV in de vorm van een cyberkeurmerk[107] (zie ook hieronder).

Oplossing op basis van de behoeftes van het mkb
63% van de geïnterviewde bedrijven maakt gebruik van een ICT-dienstverlener (zie Figuur 11). Het uitbesteden van ICT lijkt een positief effect te hebben op de cyberweerbaarheid van een bedrijf, maar het biedt geen garanties. Uit onderzoek van het DTC in 2023, blijkt dat 30% van de bedrijven ICT-veiligheidswerkzaamheden volledig uitbesteedt aan een extern bedrijf, 30% heeft eigen personeel in dienst en 24% heeft zowel eigen personeel als ICT-veiligheidswerkzaamheden uitbesteed.[108]

Uit de interviews blijkt dat bedrijven binnen het mkb, aangaande dit obstakel, behoefte hebben aan het volgende:

1. **ICT-leveranciers certificeren.** Voor ICT-leveranciers zijn certificaten beschikbaar zoals de ISO27001, maar deze worden aangeboden door commerciële partijen. Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) heeft wel toezegging gekregen voor een subsidie voor het ontwikkelen van een keurmerk voor ICT-leveranciers op het gebied van cybersecurity, maar dit gaat nog twee jaar duren. Geïnterviewden hebben ook aangegeven behoefte te hebben aan een keurmerk waarmee zij zelf weer aan hun klanten kunnen laten zien dat ze voldoende cyberweerbaarheidsmaatregelen hebben geïmplementeerd, maar dit lijkt geen breed gedragen behoefte te zijn. Door het beschikbaar stellen van een certificering of keurmerk voor ICT-leveranciers kan de kwaliteit van de geleverde diensten en producten en de betrouwbaarheid van de ICT-dienstverlener worden gewaarborgd. Hiervoor kan inspiratie gehaald worden uit het buitenland:
   - Denemarken heeft de D-seal[109], dit is een certificerings-programma voor IT-beveiliging en verantwoord gebruik van gegevens. Het is bedoeld om het beveiligingsniveau van een bedrijf te communiceren en zal vertrouwen creëren voor klanten en consumenten, en de digitale verantwoordelijkheid van bedrijven bevorderen. Het D-seal wordt uitgegeven door een onafhankelijk en private organisatie met dezelfde naam, en wordt ondersteund door onder andere de Danish Business Authority[110].
   - In Frankrijk kent men het ExpertCyber keurmerk[111]. Dit is een certificering in samenwerking met auditor AFNOR waar dienstverleners voor 800 euro, 2 jaar lang het label krijgen en in een database komen die publiekelijk toegankelijk is. Het doel hiervan is bedrijven ondersteunen in het beveiligen van informatiesystemen door gecertificeerde dienstverleners.
2. **ICT-leveranciers selecteren.** Geïnterviewden geven aan dat er een groot aanbod is aan ICT-leveranciers, met veel verschillende producten en diensten, en dat het dus lastig is te bepalen wat betrouwbare partijen zijn en welke ICT-leveranciers geschikt zijn voor het aanbieden van cybermaatregelen die passen bij het risicoprofiel van het bedrijf. Het aanbieden van een overzicht van betrouwbare ICT-leveranciers dat gevalideerd is door de overheid zou hier kunnen helpen. In hoeverre deze oplossing mogelijk is binnen de Nederlandse context vereist nader onderzoek.

[107] Zie agconnect.nl, 'Kabinet komt dit jaar nog met subsidie cyberkeurmerk ict-leveranciers', 20 sep 2023
[108] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
[109] Zie d-seal.eu
[110] Zie danishbusinessauthority.dk
[111] Zie cybermalveillance.gouv.fr, 'ExpertCyber label'

Het NCSC van het Verenigd Koninkrijk biedt iets aan op haar website dat hier invulling aan lijkt te geven, namelijk een lijst van 221 bedrijven en onderwijsinstellingen waarvan de overheid kan garanderen dat ze kwalitatieve producten en diensten leveren[112]. Dit kan gaan over commerciële producten, experts, penetratietesten, cyberincident responsediensten, cyberveiligheidsadvisering, trainingsmateriaal, etc. Verder biedt het NCSC van het Verenigd Koninkrijk het keurmerk Cyber Essentials aan[113] voor alle bedrijven. Het basiskeurmerk (Cyber Essentials) is een zelfbeoordelingsoptie die bescherming biedt tegen een breed scala aan de meest voorkomende cyberaanvallen door een reeks aan basismaatregelen aan te raden. Een tweede optie is Cyber Essentials Plus. Dit keurmerk bouwt voort op het basiskeurmerk maar vereist een uitgebreidere technische audit. Dit is dus eigenlijk een cyberveiligheidsbewijs dat gebruikt kan worden door digitale dienstverleners om kwaliteit van producten en diensten te waarborgen en aan te tonen aan potentiële klanten.

3. **Met ICT-leveranciers samenwerken.** Als bedrijven vervolgens een ICT-leverancier geselecteerd hebben, geven ze aan het lastig te vinden om de juiste vragen te stellen om zo te komen tot duidelijke onderlinge afspraken omtrent cyberweerbaarheid. Geïnterviewden geven vaak aan volledig te vertrouwen op hun ICT-leverancier en SaaS-partners in het afdekken van de risico's. Terwijl bedrijven binnen het mkb niet altijd zicht hebben op de cyberrisico's en de onderlinge verwachtingen met de ICT-leverancier niet altijd duidelijk zijn. Het opstellen van een standaard vragenlijst voor ICT-leveranciers kan hierbij helpen. Bedrijven binnen het mkb kunnen deze vragenlijst gebruiken om na te gaan in hoeverre ICT-leveranciers bepaalde cybermaatregelen hebben genomen/kunnen nemen. Dit verbetert de transparantie en communicatie tussen bedrijven binnen het mkb en ICT-leveranciers. Ook kunnen SLA's (Service Level Agreements) tussen bedrijven binnen het mkb en ICT-leveranciers helpen door duidelijke eisen over cyberveiligheid hierin mee te nemen.
4. **Groot-helpt-klein principe.** Grotere bedrijven die onder NIS2 vallen zullen strengere cybersecurity eisen moeten gaan stellen aan ketenpartners. Deze grote bedrijven kunnen hun leveranciers (vaak ook kleinere bedrijven) helpen bij het versterken van hun cyberweerbaarheid. Een voorbeeld hiervan is de 'CISO Circle of Trust (CCoT)'. Een ander voorbeeld vanuit de interviews met bedrijven binnen het mkb is een internationaal bedrijf dat sportartikelen produceert, die penetratietesten beschikbaar stelt voor leveranciers in de waardeketen. In dit specifieke geval profiteerde de mkb'er van de aangeboden penetratietest doordat fouten en gevoeligheden in het bedrijf bloot gelegd werden, waarna stappen konden worden ondernomen om de problemen op te lossen.

"Er is behoefte aan zekerheid door middel van o.a. certificeringen."
Quote van geïnterviewde mkb'er

"Omdat ISO27001 bijvoorbeeld complex is, heb ik behoefte aan een manier waarop ik kort en bondig aan klanten en leveranciers kan uitleggen/laten zien dat mijn cyberweerbaarheid op orde is en aansluit bij de risico's van het bedrijf."
Quote van geïnterviewde mkb'er

"Maak het pragmatisch door bijvoorbeeld een checklist te maken die voorgelegd kan worden bij de IT-dienstverlener om te valideren of de cyberdiensten die ze leveren voldoende zijn; maak het niet te groot of te ingewikkeld."
Quote van geïnterviewde mkb'er

5.4.7 Obstakel 7: Beperkte vindbaarheid van (overheids-) hulpmiddelen

Het huidige aanbod van de hulpmiddelen
Voor het obstakel 'Beperkte vindbaarheid van (overheids-) hulpmiddelen' wordt er één hulpmiddel aangeboden vanuit de overheid. Dit is de Wegwijzer voor Cybersecurity Initiatieven van het DTC (zie Tabel 4). Daarnaast worden er geen hulpmiddelen aangeboden via samenwerkingsverbanden (zie Tabel 5).

Uitdagingen met betrekking tot het aanbod van de hulpmiddelen
Dit obstakel kan vanuit twee perspectieven worden bekeken: het bedrijf binnen het mkb, en de aanbieder van hulpmiddelen, in dit geval het DTC, de KVK en het NCSC.

Bedrijven binnen het mkb. 9% van de geïnterviewden geeft aan bekend te zijn met het DTC en/of het NCSC (zie Figuur 11). Uit onderzoek van het DTC blijkt dit 20% te zijn.[114] Het hulpmiddel 'Wegwijzer voor Cybersecurity Initiatieven' van het DTC kan dan waardevol zijn, maar niet voor de bedrijven die het DTC überhaupt niet weten te vinden. Het obstakel 'Vindbaarheid van (overheids-)initiatieven' lijkt dus vanuit de geïnterviewden meer te gaan over bekendheid met relevante partijen zoals het DTC en NCSC en de rol die ze spelen. Dit punt raakt daarmee ook aan 5.4.1 waarin gesproken wordt over de positionering van het DTC/NCSC. Overigens geeft 16% van de geïnterviewden aan online hulpmiddelen op te zoeken voor het verbeteren van hun cyberweerbaarheid (zie Figuur 11). Het lijkt dat het probleem niet ligt in het aanbod en de vindbaarheid van online hulpmiddelen, maar dat er überhaupt weinig naar gezocht wordt. Op basis van de gesprekken met de geïnterviewden lijkt een gebrek aan bewustzijn een belangrijke oorzaak hiervoor. Bedrijven beseffen onvoldoende dat de overheid een actieve rol neemt rondom cyberveiligheid, en dat ze daar terecht kunnen voor hulp. Dit betekent overigens niet dat er geen verbeteringen mogelijk zijn in het aanbod en de vindbaarheid van de hulpmiddelen; dit wordt meegenomen als onderdeel van de mogelijke oplossingen.

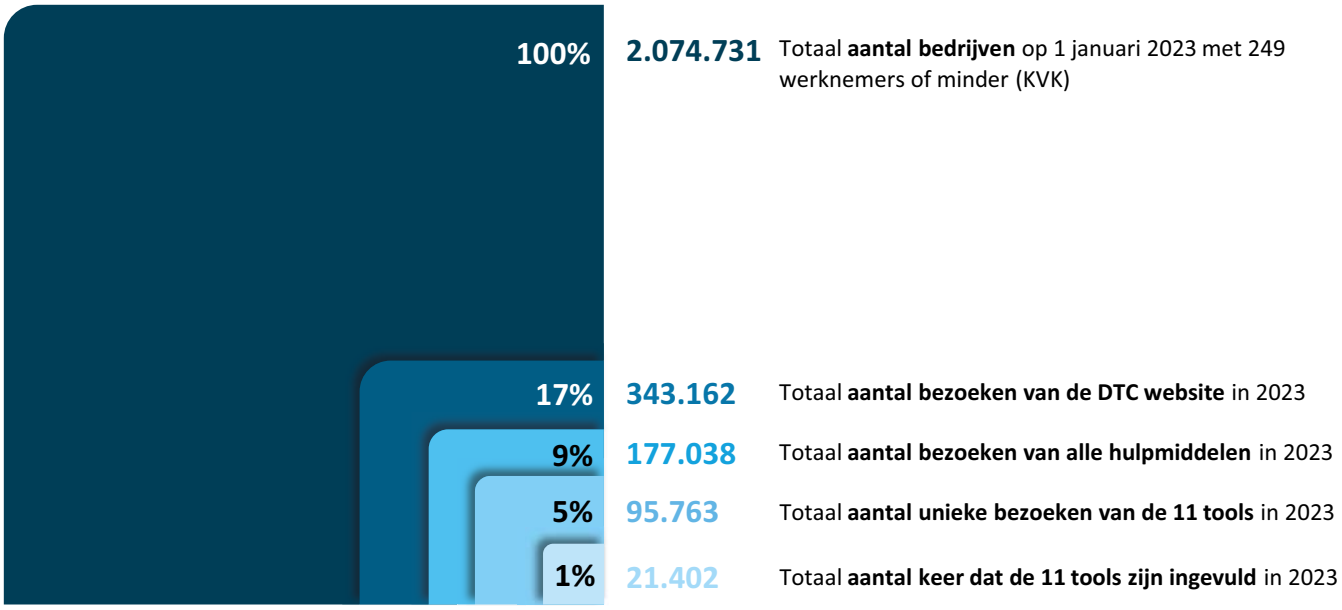
[112] Zie ncsc.gov.uk, 'Verify suppliers'
[113] Zie ncsc.gov.uk, 'Cyber Essentials'
[114] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023

"Je hebt kennis nodig [voor cybersecurity]; ik wil dit wel regelen maar ik zou niet weten hoe. Waar vind ik tips over cyber?"
Quote van geïnterviewde mkb'er

Aanbieder van hulpmiddelen: het DTC. Het DTC vervult een sleutelpositie in het Nederlandse cyberlandschap en biedt veel informatie en hulpmiddelen aan die waardevol zijn voor bedrijven binnen het mkb. Om deze rol effectief te vervullen is het belangrijk dat het DTC zichtbaar is voor bedrijven, dat haar rol en toegevoegde waarde bekend is bij de gebruikers van de hulpmiddelen, en dat de hulpmiddelen voorzien in de behoefte van bedrijven binnen het mkb. De zichtbaarheid of bekendheid van het DTC lijkt elk jaar toe te nemen, afgaande op het aantal bezoeken van de website (zie Figuur 14).

Figuur 7 geeft een beter beeld van de absolute bekendheid en de vindbaarheid van de hulpmiddelen van het DTC aan de hand van data aangeleverd door het DTC (zie Tabel 16 in Appendix G – Gegevens DTC). De data laat met name zien hoe vaak een bepaalde webpagina, hulpmiddel of tool van het DTC bezocht is. De data is aangeleverd voor de periode van 1 januari tot en met 15 november 2023. Om een beeld te krijgen van het gehele jaar zijn deze waardes geëxtrapoleerd voor Figuur 7. Deze informatie is vervolgens gerelateerd aan het totaal aantal bedrijven binnen het mkb. Volgens de KVK waren dat er op 1 januari 2023 2.074.731; dit zijn dus alle bedrijven in Nederland met 249 werknemers of minder. Voor het meest positieve scenario wordt aangenomen dat elk bezoek aan de website een uniek bedrijf binnen het mkb is. De figuur laat voor dit scenario zien dat 17% van alle bedrijven binnen het mkb het DTC vindt, 9% gebruik maakt van de hulpmiddelen, 5% gebruik maakt van de tools, en 1% de tools volledig invult.

Bekendheid en vindbaarheid van het DTC en de hulpmiddelen
Geïllustreerd aan de hand van data over websitegebruik



Figuur 7 Bekendheid van het DTC aan de hand van het aantal websitebezoeken uitgezet tegen het totaal aantal bedrijven binnen het mkb.

Aanbieder van hulpmiddelen: de KVK. De Kamer van Koophandel (KVK) vervult een belangrijke positie in het cyberlandschap gezien het zicht heeft op en in nauw contact staat met bedrijven binnen het mkb. De KVK biedt op haar website ook verschillende hulpmiddelen aan rondom cyberveiligheid. De KVK geeft schriftelijk aan dat uit eigen onderzoek blijkt dat ongeveer 7% van de ondernemers informatie zoekt over cyberveiligheid, waarvan de helft (3%) hiervoor de KVK gebruikt.

Aanbieder van hulpmiddelen: het NCSC. Het Nationaal Cyber Security Centrum (NCSC) heeft een belangrijke rol, hoewel deze in vergelijking met het DTC, in mindere mate gericht is op bedrijven binnen het mkb. Haar activiteiten zijn overkoepelend, met een focus op het begrijpen van kwetsbaarheden en dreigingen, het verbinden van (inter)nationale partners, kennis en informatie, en het voorkomen van maatschappelijke schade en beperken van dreigingen[115]. Dit twee-partijen model is overigens vergelijkbaar met de situatie in Frankrijk.

[115] Zie ncsc.nl

Het NCSC heeft eveneens schriftelijk aantallen gedeeld over de top 10 zoektermen op de website en de top 15 kennisproducten (zie Tabel 17). Geëxtrapoleerd voor het gehele jaar 2023 (365 dagen) zijn de totale aantallen 26.228 bezoeken (zoektermen + kennisproducten), het is niet duidelijke hoeveel van deze bezoeken van bedrijven binnen het mkb zijn. Het NCSC geeft aan dat, met betrekking tot de kennisproducten, bedrijven binnen het mkb niet een doelgroep is waar het NCSC zich op richt.

Het NCSC heeft ook informatie gedeeld over het hulpmiddel veiliginternetten.nl. Voor de periode van januari – juni 2023 was het aantal bezoekers van deze website 350.000; extrapolerend voor het gehele jaar betekent dit een totaal aantal van 700.000. Het NCSC geeft aan dat de website in de huidige staat niet gericht is op ondernemers; de website bevatte wel informatie voor ondernemers, maar deze is overgedragen aan het DTC bij haar oprichting in 2018.

Evaluatie effectiviteit van hulmiddelen. Op basis van het contact met de aanbieders van hulpmiddelen (DTC, KVK, NCSC) is er ook gekeken naar het gebruik en de effectiviteit van hulpmiddelen. Want wanneer bedrijven binnen het mkb de hulpmiddelen vinden, betekent dit niet dat bedrijven deze hulpmiddelen ook gebruiken of dat ze effectief zijn.

Zoals hierboven beschreven houdt het DTC het aantal bezoeken van de webpagina's en hulpmiddelen bij, waarbij onderscheid wordt gemaakt tussen het totale aantal en de unieke bezoeken. Verder houdt het DTC van de 11 tools (CyberVeilig Check, etc.) bij of de tool wordt gestart en of deze wordt ingevuld. Hiermee is inzichtelijk te maken of een tool gevonden en daadwerkelijk gebruikt wordt. Als voorbeeld is de CyberVeilig Check in 2023 (zie Tabel 16 in Appendix G – Gegevens DTC):

- 58.284 unieke keren bezocht (100%);
- 8.012 keren gestart (13,7%);
- 6.258 keren ingevuld (10,7%).

Gebruikers kunnen voor sommige tools feedback achterlaten in de vorm van een score tussen de 0 en 5 sterren, of door middel van een like/dislike. Voor de 11 tools laat 3% (738 van de 21.402; Tabel 16 in Appendix G – Gegevens DTC) van de gebruikers die de tools invullen een review achter. Naast de standaard reviewmogelijkheden via de website wordt er ook feedback opgehaald via de DTC Community en worden hulpmiddelen ook getoetst met deze community voordat ze breder gedeeld worden.

De KVK verzamelt wel kwalitatieve en kwantitatieve feedback maar het is onduidelijk in welke vorm deze feedback opgehaald wordt. Het NCSC geeft aan kwalitatieve feedback op te halen over kennisproducten bij partijen binnen de vitale infrastructuur, maar geen kwantitatieve effectmetingen te doen.

Voor zover er kwantitatieve effectmetingen plaatsvinden bij publieke aanbieders van hulpmiddelen, geven deze enkel inzicht in de waardering van het hulpmiddel door de gebruiker. Deze informatie is wel een indicator voor hoe goed een hulpmiddel werkt, maar geeft geen sluitend antwoord op de vraag of een hulpmiddel effectief is in het oplossen van een obstakel. Kwalitatieve feedback kan hier wel meer inzicht in bieden, maar in hoeverre deze feedback verzameld wordt en wat de kwaliteit ervan is, is onduidelijk.

Oplossing op basis van de behoeftes van het mkb

Bedrijven binnen het mkb. Geïnterviewden geven aan behoefte te hebben aan:

1. **Wegwijzer cyberveiligheid aanbieden.** Er is behoefte aan een duidelijke en complete wegwijzer als het gaat om allerhande onderwerpen rondom cyberveiligheid. Dit is breder dan de wegwijzer van het DTC; het gaat om een antwoord op de vraag bij wie bedrijven moeten zijn, en welke hulp ze van die partij kunnen verwachten. Er zijn namelijk veel tools en hulpmiddelen beschikbaar, het is alleen niet duidelijk wie wat aanbiedt.
2. **Centraal punt met hulplijn opzetten.** Er is behoefte aan één centraal punt waar alles verzameld is (informatie, hulpmiddelen, advies, uitleg, etc.), en ook gedeeld wordt. Op deze manier kan iemand die op zoek is naar informatie, erop vertrouwen dat dit centrale punt alle informatie biedt. En indien een bepaalde dienst/hulpmiddel wordt aangeboden door een andere partij, moet er een doorverwijzing zijn naar die partij (zie ook 'Wegwijzer cyberveiligheid aanbieden' hierboven); dit kan in de vorm van een loket dat als aanspreekpunt fungeert binnen het complexe Nederlandse cyberlandschap.
   Ook is er behoefte aan de mogelijkheid om dit centrale punt te bellen voor advies en ondersteuning omtrent cyberweerbaarheidsvraagstukken. Een voorbeeld van hoe andere landen een hulplijn inrichten is de 'cyberhotline' van de Deense organisatie 'sikkerdigital.dk' . Dit is een samenwerking tussen onder andere de 'Danish Agency for Digitalisation', het Deense NCSC en andere partners. De organisatie biedt onder andere een cyberhotline aan voor burgers en bedrijven die advies en begeleiding nodig hebben in het geval van digitale fraude en cyberaanvallen. Het telefoonnummer kan voor algemene vragen elke werkdag gebeld worden tussen 08:00 en 20:00, en in het weekend tussen 10:00 en 16:00; voor dringende vragen over identiteitsfraude of cyberaanvallen is het telefoonnummer 24/7 beschikbaar. Frankrijk biedt een vergelijkbare dienst via nationale 'Computer Emergency Response Team' (CERT-FR) dat 24/7 fungeert als het contactpunt voor alle cyberincidenten[117]. Het CERT-FR richt zich met name op publieke organisaties en vitale organisaties, niet het brede Franse publiek of het mkb, hiervoor bestaat Cybermalveillance[118]. Dit publiek-private platform verwijst onder andere door naar de politie waarmee het mogelijk is 24/7 contact op te nemen via een online chatdienst.

[116] Zie sikkerdigital.dk/cyberhotline
[117] Zie cert.ssi.gouv.fr, 'About CERT-FR'
[118] Zie cybermalveillance.gouv.fr

Samenvattend dient dit centrale punt de volgende functionaliteit te hebben:

- Centraal (publiek-privaat) loket binnen het gehele cyberlandschap;
- Wegwijzer richting andere relevante partijen/hulpmiddelen binnen het cyberlandschap;
- Kennisbank met een toegespitste en gestructureerde verzameling van allerhande uniforme, betrouwbare en begrijpelijke informatie en hulpmiddelen (denk aan: cyberweerbaarheidsmaatregelen, investeringswijzer, nationale en internationale wet- en regelgeving, NIST-framework, NIS2, tools voor het bepalen van het risicoprofiel en huidige cyberweerbaarheidsniveau, etc.);
- Bron van advies en ondersteuning, door middel van bijvoorbeeld een hulplijn.

Wat opvalt is dat de twee bovengenoemde genoemde behoeftes vanuit de geïnterviewden al deels afgedekt worden door het DTC; het lijkt alleen dat bedrijven hiervan niet op de hoogte zijn. Uit de eerder gedeelde data blijkt dat het grootste gedeelte van de geïnterviewden geen gebruik maakt van de hulpmiddelen vanuit de overheid (9%, zie Figuur 11), hierdoor zal een groot deel niet beseffen dat er voor sommige behoeftes al hulpmiddelen worden aangeboden.

Aanbieders van hulpmiddelen.

1. **Het NCSC en DTC positioneren.** Voor bedrijven binnen het mkb, maar ook voor andere partijen zoals brancheorganisaties, belangenverenigingen, etc., moet duidelijk zijn wie welke rol heeft in het Nederlandse cyberlandschap. Een duidelijke rol vanuit het NCSC en DTC helpt bij het verbeteren van de vindbaarheid van hulpmiddelen en bij het faciliteren en stimuleren van verbindingen tussen partijen. Een belangrijke eerste stap is al genomen door het samenvoegen van het NCSC, DTC en Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) in een centraal expertisecentrum in 2026[119]. Hierbij valt er veel te leren van de Nationale Cyber Security Centra in het Verenigd Koninkrijk en Frankrijk.
   a. In het Verenigd Koninkrijk heeft het NCSC een centrale rol, en zijn de taken[120] gekoppeld aan de overkoepelende ambitie om als Verenigd Koninkrijk een van de meest veilige en aantrekkelijke digitale economieën te zijn om in te wonen, zaken te doen en te investeren[121]. Additioneel heeft het NCSC in het Verenigd Koninkrijk een 'actieve, hands-on approach' door bijvoorbeeld de kennis die ze deelt toe te spitsen op verschillende doelgroepen (individuen en families, zzp, mkb, grootbedrijven, publieke sector, cyberveiligheidsexperts), advies en richtlijnen aan te bieden per sector (agricultuur, bouw, onderwijs, etc.), en een uitgebreide lijst aan producten aan te bieden (Cyber Assessment Framework, Verify a supplier, NCSC certification, etc.).
   b. In Frankrijk lijkt de positionering van (inter)nationale overheidsorganisaties ook sterk. Waar de Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)[122] meer gericht is op (inter)nationale vraagstukken rond cyberveiligheid, is Cybermalveillance een publiek-privaat platform dat allerlei partijen, verticaal en horizontaal, met elkaar verbindt. Naast allerhande praktische hulpmiddelen is het bijvoorbeeld mogelijk 24/7 contact op te nemen met Cybermalveillance die je op basis van je vraag doorverbindt met de juiste partij.
   c. Het NCSC, DTC en Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) in Nederland worden al samengevoegd in 2026[123], en hier ligt dus ook een kans om het centrale expertisecentrum goed en herkenbaar te positioneren in de samenleving, zodat ook bedrijven binnen het mkb deze organisatie weten te vinden. Daarnaast kan er naar voorbeeld van het VK een sterke, zichtbare connectie zijn met overkoepelende strategieën zoals de Nationale Cybersecurity Strategie en de Kabinetsstrategie Digitale Economie[124].
2. **Inhoud van de hulpmiddelen uniformeren.** Er worden al veel hulpmiddelen aangeboden door het DTC, de NCSC en de KVK, maar er mist structuur, samenhang, synergie tussen de hulpmiddelen. Een simpel voorbeeld: zowel het NCSC[125], het DTC[126] en de KVK[127] bieden informatie aan over basismaatregelen voor cyberveiligheid. De 8 maatregelen van het NCSC richten zich op "elke organisatie" en gaan van risicomanagement, naar versleuteling, naar het centraliseren van loginformatie. De 7 maatregelen van het DTC zijn gericht op "elk bedrijf" hoewel de pagina wel doorverwijst naar de CyberVeilig Check voor zzp en mkb. Hoewel de maatregelen van het NCSC en DTC deels overlappen zijn er zeker verschillen, zoals het gebruik van antivirussoftware. Als laatste biedt de KVK 10 maatregelen aan "om veilig online te ondernemen" met maatregelen die vergelijkbaar zijn met die van het DTC. Opvallend hier is dat de KVK adviseert om bij vragen contact op te nemen met de IT-dienstverlener, een cyberveiligheidsexpert of het KVK-adviesteam middels een telefoonnummer en live chat. Verder is de KVK de enige die aangeeft wanneer de informatie is bijgewerkt. Dit brede, kwalitatieve aanbod van informatie en handelingsperspectief is waardevol, maar de keerzijde kan zijn dat bedrijven binnen het mkb niet weten waar ze moeten beginnen of bij wie ze moeten zijn, niet weten of de informatie volledig is, of door de bomen het bos niet meer zien. Een grote stap naar verbetering kan dus worden gemaakt door het verzamelen en bundelen van de hulpmiddelen vanuit de overheid om structuur, samenhang en synergie te creëren. Het geheel aan hulpmiddelen, expertises en organisaties vormt zo een centrale en bruikbare kennispool voor het mkb.

[119] Zie NCSC.nl, 'Nationale cybersecurity organisaties gaan krachten bundelen', 7 september 2022
[120] Zie NCSC.gov.uk, 'What we do'
[121] HM Government, 'Government Cyber Security Strategy 2022-2030'
[122] Zie cyber.gouv.fr, 'About ANSSI'
[123] Zie NCSC.nl, 'Nationale cybersecurity organisaties gaan krachten bundelen', 7 september 2022
[124] Zie DTC.nl, 'Kabinetsstrategie Digitale Economie: versterk cybersecurity', 26 oktober 2023
[125] Zie ncsc.nl, 'Basismaatregelen cybersecurity'
[126] Zie digitaltrustcenter.nl, 'Starten met cybersecurity? Begin met deze maatregelen'
[127] Zie kvk.nl, 'Werk jij digitaal veilig? Controleer het met de checklist'

3. **Hulpmiddelen structureel evalueren.** Uit de data die is aangeleverd door het DTC, NCSC en de KVK, blijkt dat de hulpmiddelen op dit moment nog onvoldoende worden geëvalueerd op basis van de effectiviteit. Het is van belang om inzichtelijk te maken in hoeverre een hulpmiddel daadwerkelijk bijdraagt aan het verbeteren van het cyberweerbaarheidsniveau van bedrijven binnen het mkb; dit dient gedaan te worden samen met deze bedrijven. Zo wordt ook voorkomen dat er continu nieuwe hulpmiddelen worden ontwikkeld zonder dat er aandacht is voor het verbeteren van de huidige hulpmiddelen. Dit zouden de aanbieders van hupmiddelen op een structurele basis kunnen doen om continue verbetering te waarborgen.

5.4.8 Obstakel 8: Veranderend dreigingslandschap

Het huidige aanbod van de hulpmiddelen
Voor obstakel 8, 'Veranderend dreigingslandschap', worden er geen hulpmiddelen aangeboden vanuit de overheid of private partijen. Daarnaast worden er ook geen hulpmiddelen aangeboden via samenwerkingsverbanden (zie Tabel 4 en Tabel 12).

Uitdagingen met betrekking tot het aanbod van de hulpmiddelen
Slechts één van de geïnterviewden geeft aan moeite te hebben met dit obstakel en noemt dat "dreigingen steeds geavanceerder worden", maar noemt geen behoeftes die hier verder op in gaan. Enkele anderen noemen bijvoorbeeld nog wel kunstmatige intelligentie en veranderende technologieën zoals ChatGPT als factor waardoor het moeilijker zal worden cyberweerbaar te zijn, maar noemen hier ook geen concrete behoeftes.

Het veranderende dreigingslandschap is een breed, maatschappelijk probleem dat meer relevant is voor de gehele samenleving. Maar met name handhavende partijen zoals de Nationale Politie, Ministerie van Defensie of het Openbaar Ministerie zullen dit moeten monitoren om de cyberweerbaarheid van heel Nederland te versterken. Het feit dat er geen hulpmiddelen zijn gevonden voor bedrijven binnen het mkb, het obstakel nauwelijks genoemd wordt door geïnterviewden en er ook geen directe behoeftes voor zijn, schetst het beeld dat dit obstakel verder van bedrijven binnen het mkb af staat vergeleken met de andere obstakels.

Oplossing op basis van de behoeftes van het mkb
Vanuit de interviews met bedrijven binnen het mkb zijn er geen specifieke behoeftes geuit voor het oplossen van een veranderend dreigingslandschap. Een mogelijke reden hiervoor is dat bedrijven binnen het mkb dit obstakel niet zien als iets waar ze zelf invloed op kunnen uitoefenen. Een behoefte die bedrijven wel hebben geuit is de vraag naar inzicht in data waarmee een beeld wordt geschetst van de omvang van het dreigingslandschap. Dit kunnen bijvoorbeeld statistieken zijn over het aantal cyberincidenten in Nederland, de kosten van de cyberincidenten per sector en het percentage startups dat gehackt wordt, etc.

6. Mogelijkheden om te komen tot een metriek

6. Mogelijkheden om te komen tot een metriek

6.1 Definitie metriek

In de context van dit onderzoek is een metriek gedefinieerd als een meetinstrument dat een objectieve, kwantitatieve score produceert van de cyberweerbaarheid van een bedrijf, op basis van indicatoren die betrekking hebben op het voorkomen, identificeren, reageren en herstellen (incl. het leervermogen) van cyberaanvallen[128]. In de literatuur wordt er ook wel gerefereerd naar 'volwassenheidsmodellen'[129]. Een volwassenheidsmodel is een set van kenmerken, indicatoren of patronen die gekoppeld zijn aan volwassenheidsniveaus in een bepaald domein of discipline[130]. In het onderzoek is dit domein cyberweerbaarheid.

6.2 Doel metriek

Het doel van het ontwikkelen van een metriek is dat het de mogelijkheid biedt een beoordeling te geven van het huidige en optimale cyberweerbaarheidsniveau van een organisatie. Bij veel metrieken wordt het optimale niveau uitgedrukt in een volwassenheidsniveau. Echter om het optimale niveau te bepalen dienen eerst de risico's in kaart gebracht te worden. Dit kan door middel van een risicoanalyse. Een risicoanalyse is een methode om inzicht te krijgen in de risico's die een bedrijf loopt. Hierbij wordt er gekeken naar de kans dat iets gebeurt en de gevolgen als dat gebeurt (impact).[131] Een risicoanalyse houdt hierin rekening met de bedrijfsdoelstellingen, dreigingen, kwetsbaarheden, en potentiële impact van cyberincidenten binnen het bedrijf[132]. De stappen die doorlopen kunnen worden om het huidige en optimale cyberweerbaarheidsniveau te bepalen zijn:

- In kaart brengen van het huidige cyberweerbaarheidsniveau (metriek);
- Beoordelen van de belangrijkste risico's (risicoanalyse);
- Definiëren van het optimale cyberweerbaarheidsniveau (metriek);
- Bepalen welke maatregelen genomen dienen te worden om tot het optimale cyberweerbaarheidsniveau te komen (metriek).

De volgorde van de bovengenoemde stappen kan verschillen gezien, bijvoorbeeld, stappen 1 en 2 omgewisseld kunnen worden. Belangrijk is uiteindelijk dat de maatregelen genomen worden.

6.3 Voorwaarden metriek voor bedrijven binnen het mkb

Binnen het thema cyberweerbaarheid zijn er verschillende metrieken beschikbaar; zoals het Cybersecurity Capability Maturity Model (C2M2) en de NIST Maturity Assessment tool. Echter blijkt uit de interviews met de bedrijven binnen het mkb dat deze metrieken vaak lastig te interpreteren zijn voor bedrijven met minder cybersecurity kennis en expertise waardoor vaak externe experts de mkb'ers moeten ondersteunen. Dit vraagt een extra investering waardoor bedrijven ontmoedigd worden om een metriek te gaan gebruiken. Daarnaast bevatten de metrieken vaak algemene kaders en zijn deze beter toepasbaar voor grotere bedrijven en minder geschikt voor kleinere bedrijven.

Op basis van de interviews met de bedrijven binnen het mkb en validatie binnen de literatuur is er in dit onderzoek een aantal voorwaarden opgesteld voor het hanteren van een metriek voor bedrijven binnen het mkb:

- De metriek dient pragmatisch te zijn (praktisch en doelmatig);
- De metriek dient toepasbaar te zijn voor bedrijven binnen het mkb;
- De metriek dient gratis of tegen een gereduceerd tarief te worden aangeboden;
- De metriek dient genoeg handelingsperspectief te bieden en geeft aan wat het huidige cyberweerbaarheidsniveau is en de mogelijkheden om te komen tot een optimaal niveau.

6.4 Evaluatie huidige metriek

Om tot een evaluatie te komen van de huidige metrieken, dienen deze eerst in kaart gebracht te worden . Het overzicht van de huidige metrieken staat in Tabel 7.

Metriek	Land
BIO Self-Assessment (BIO-SA) (CIP)	Nederland
Handreiking bij volwassenheidsmodel Informatiebeveiliging (NBA)	Nederland
3-Pijlermodel (Spruit)	Nederland
Risicoklassenindeling Digitale Veiligheid (DTC)	Nederland
CyberVeilig Check (DTC)	Nederland
Basisscan Cyberweerbaarheid (DTC)	Nederland
CYRA (CyberRating)	Nederland
NIST Information Security Maturity Model (NIST)	Verenigde Staten
Cybersecurity Capability Maturity Model (C2M2)	Verenigde Staten
Information Security Management System (ISMS) Maturity Capability Model	Verenigde Staten
Open Group's Information Security Management Maturity Model	Verenigde Staten

Tabel 7 Overzicht van metrieken en land van herkomst.

[128] Definitie bepaald op basis van afstemming met CSR
[129] Analyse volwassenheidsmodellen voor informatiebeveiliging, Informatiebeveiliging Magazine – De Haagse Hogeschool
[130] Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for Nist Cyber Security Framework. Computer Science & Information Technology (CS&IT), 7(3), 51-62
[131] https://cyberveilignederland.nl/woordenboek
[132] Stappenplan risicoanalyse, Digital Trust Center
[133] Analyse volwassenheidsmodellen voor informatiebeveiliging, Informatiebeveiliging Magazine – De Haagse Hogeschool
[134] Information Security Management Maturity Models (2022). Procedia Computer Science. Volume 213, 49-57

Onderstaande metrieken zijn getoetst op basis van deskresearch en de voorwaarden die zijn opgesteld (zie 6.3).

Metriek	Evaluatie
BIO Self-Assessment (BIO-SA) (CIP)	• Gebaseerd op NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. • Biedt een volledig overzicht van de te nemen maatregelen. • Gericht op overheidsorganisaties dus minder geschikt voor het mkb.
Handreiking bij volwassenheids-model Informatiebeveiliging (NBA)	• Gebaseerd op NIST, BIO, DNB, ISO en CoBIT . • Biedt een volledig overzicht van de te nemen maatregelen; deze zijn geclusterd in aandachtsgebieden. • Geeft een duidelijk beeld van het huidige niveau, optimale niveau en de te nemen maatregelen.
3-Pijlermodel (Spruit)	• Overzichtelijk en gestructureerd aan de hand van 3 pijlers: de goede dingen doen, de dingen goed doen en de dingen goed beleggen. Ook de lijst met vragen die gesteld worden is vrij overzichtelijk. • Het analyseschema en de berekening om het huidige en optimale niveau te bepalen zijn vrij complex.
Risicoklassenindeling Digitale Veiligheid (DTC)	• Overzichtelijk, toegankelijk en makkelijk in te vullen door bedrijven. • Specifiek gericht op bedrijven binnen het mkb dus goed toepasbaar. • Geeft alleen het optimale cyberweerbaarheidsniveau weer passend bij het risicoprofiel van het bedrijf en een set aan bijbehorende maatregelen. Geeft dus niet het huidige niveau van het bedrijf weer.
CyberVeilig Check (DTC)	• Overzichtelijk, toegankelijk en makkelijk in te vullen door bedrijven. • Specifiek gericht op bedrijven binnen het mkb dus goed toepasbaar. • Geeft alleen het huidige cyberweerbaarheidsniveau weer en een set aan bijbehorende maatregelen maar houdt niet rekening met het optimale niveau van het bedrijf.
Basisscan Cyberweerbaarheid (DTC)	• Overzichtelijk, toegankelijk en makkelijk in te vullen door bedrijven. • Specifiek gericht op bedrijven binnen het mkb dus goed toepasbaar. • Geeft alleen het huidige cyberweerbaarheidsniveau weer en een set aan bijbehorende maatregelen maar houdt niet rekening met het optimale niveau van het bedrijf.
CYRA (CyberRating)	• Is gericht op bedrijven binnen het mkb maar alleen toegankelijk voor bedrijven die lid zijn van samenwerkingsverbanden die aangesloten zijn bij de CYRA. • Het bedrijf dat de CYRA invult is zelf verantwoordelijk voor het bepalen van het optimale cyberweerbaarheidsniveau op basis van hun risicoprofiel. De CYRA helpt hier wel bij door het bieden van een korte vragenlijst van 9 vragen omtrent integriteit, vertrouwelijkheid en beschikbaarheid. • Stelt het huidige cyberweerbaarheidsniveau vast aan de hand van een self-assessment met vragen die gebaseerd zijn op de ISO27001/2, ISO27701, GDPR, NBA volwassenheidsmodel en CMM + CMMC. • Bedrijven krijgen alleen inzicht in de te nemen cybermaatregelen door de vragenlijst door te nemen, er wordt nog geen rapport beschikbaar gesteld. Deze mogelijkheid is nog in ontwikkeling. • Biedt als vervolgstap een CYRA audit aan om te valideren in hoeverre de self-assessment klopt. Dit is een betaalde dienst die wordt aangeboden vanuit TÜV Nord Nederland en afhankelijk van het lidmaatschap van het samenwerkingsverband dient een bedrijf hier zelf voor te betalen of niet.
NIST Information Security Maturity Model (NIST)	• Biedt een volledig overzicht van de te nemen maatregelen, deze zijn geclusterd aan de hand van de processtappen: identificeren, beschermen, detecteren, reageren, herstellen. • Geeft een duidelijk beeld van het huidige niveau, optimale niveau en de te nemen maatregelen. • Uitgebreide metriek waardoor ondersteuning van externe experts mogelijk nodig is voor het mkb.
Cybersecurity Capability Maturity Model (C2M2)	• Biedt een volledig overzicht maatregelen gericht op zowel Information Technology (IT) als Operations Technology (OT). • Geeft alleen het huidige cyberweerbaarheidsniveau weer en de te nemen maatregelen om dit te verbeteren maar geeft geen inzicht in het optimale cyberweerbaarheidsniveau. • Gericht op de energie sector dus alleen geschikt voor een deel van de bedrijven binnen het mkb.
Information Security Management System (ISMS) Maturity Capability Model	• Beoordeelt de volwassenheid van de cybersecurity processen die van invloed zijn op de ISMS'en van een organisatie. • Geeft alleen het huidige cyberweerbaarheidsniveau weer maar geeft geen inzicht in het optimale cyberweerbaarheidsniveau. • Abstract en lastig toepasbaar voor het mkb want metriek focust op de evaluatie van processen en minder op concrete maatregelen.
Open Group's Information Security Management Maturity Model	• Gebaseerd op ISO9001, COBIT, ITIL, ISO/IEC 27000. • Belangrijkste doel is om investeringen in cybersecurity te prioriteren en optimaliseren. • Beoordeelt de volwassenheid van de cybersecurity processen die van invloed zijn op de ISMS'en van een organisatie. • Hoog kennisniveau benodigd voor toepassen metriek waardoor ondersteuning van externe experts mogelijk nodig is.

Tabel 8 Evaluatie van de metrieken langs verschillende variabelen.

[135] Zie cyberrating.nl

6.5 Conclusie

Er is behoefte aan een metriek om op een uniforme wijze het huidige en optimale cyberweerbaarheidsniveau voor bedrijven binnen het mkb inzichtelijk te maken en maatregelen voor verbetering te identificeren. Deze maatregelen dienen bedrijven binnen het mkb concreet handelingsperspectief te bieden. De enige metrieken die zich specifiek richten op het mkb zijn de CyberVeilig Check, de Basisscan Cyberweerbaarheid, de CYRA en de Risicoklasse Tool.

Alleen de CYRA biedt inzicht in zowel het huidige als het optimale cyberweerbaarheidsniveau en stelt het optimale cyberweerbaarheidsniveau vast op basis van een korte vragenlijst waarin het risicoprofiel van het bedrijf wordt geschetst. Echter geven bedrijven binnen het mkb aan dat ze juist behoefte hebben aan hulp bij het inzichtelijk maken van de risico's om zo een passend optimaal cyberweerbaarheidsniveau te bepalen en handelingsperspectief te bieden dat hierbij aansluit (zie 5.4.2 Obstakel 2: Onvoldoende inzicht in risico's en handelingsperspectief). Een vragenlijst van 9 vragen is mogelijk niet voldoende hulp voor het mkb. Een mogelijke oplossing zou zijn om losse risico analyse te koppelen aan de volwassenheidsniveaus die de CYRA (of een andere metriek) voorschrijft.

Uit de evaluatie van de metrieken blijkt dat er meerdere mogelijkheden zijn voor het in kaart brengen van het huidige en optimale cyberweerbaarheidsniveau. Bedrijven binnen het mkb kunnen deze metriek zelf invullen of laten invullen door een onafhankelijke partij (bijvoorbeeld een IT-auditor of accountant). Dit onderzoek geeft de mogelijke opties weer maar geeft geen uitsluitsel over wat de meest geschikte metriek is voor bedrijven binnen het mkb. Er zal een vervolgonderzoek nodig zijn om dieper in te gaan op de verschillende mogelijkheden en om dit ook te toetsen bij bedrijven binnen het mkb.

7. Conclusies en aanbevelingen

7. Conclusies en aanbevelingen

Dit rapport geeft antwoord op de volgende onderzoeksvragen:

Hoofdvraag 1

Hoofdvraag 1: Waarom is er een cyberweerbaarheidskloof en welke mogelijkheden zijn er voor bedrijven om hun cyberweerbaarheidsniveau in kaart te brengen?
Subvraag 1: Wat zijn mogelijke verklaringen voor een suboptimaal cyberweerbaarheidsniveau bij bedrijven (in termen van onderinvestering)?
Antwoord subvraag 1: Er zijn **acht obstakels geïdentificeerd** die bedrijven binnen het mkb ervan weerhouden hun cyberweerbaarheidsniveau te versterken naar een voor hen optimaal niveau (dat wil zeggen: afgestemd op het risicoprofiel). Bedrijven die relatief ver van hun optimale niveau afzitten, vormen de groep achterblijvers. **De achterblijvers** weten niet wat hun huidige en optimale niveau is, of hebben hier wel inzicht in maar kunnen of willen bewust niet verbeteren om te komen tot hun optimale niveau. De acht obstakels bevatten **drie interne obstakels** waar het bedrijf direct invloed op heeft:

1. Onvoldoende cyberbewustzijn en -kennis;
2. Onvoldoende inzicht in risico's en handelingsperspectief;
3. Lastig te bepalen hoeveel en waarin moet worden geïnvesteerd.

Daarnaast zijn er **vijf externe obstakels** waar bedrijven nauwelijks of geen invloed op hebben maar wel de gevolgen van ervaren:

1. Algemeen tekort aan personeel in Nederland met expertise in ICT en cyberveiligheid;
2. Beperkte toepasbaarheid huidige richtlijnen voor het mkb;
3. Afhankelijkheidsrisico's in toeleveringsketen;
4. Beperkte vindbaarheid van (overheids-)hulpmiddelen;
5. Veranderend dreigingslandschap.

Er is samenhang tussen de obstakels. Dit betekent dat obstakels elkaar onderling kunnen versterken, maar ook dat er een bepaalde volgordelijkheid is; dit laatste is voornamelijk zichtbaar bij de interne obstakels:

- 'Onderinvestering' kan bijvoorbeeld voortkomen uit onduidelijkheid over hoeveel en in welke cybersecurityoplossingen (obstakel 3) geïnvesteerd moet worden om tot een optimaal cyberweerbaarheidsniveau te komen;
- Deze onduidelijkheid kan weer voortkomen uit een beperkt inzicht in wat de risico's voor een bedrijf zijn en de beschikbare mogelijkheden om te handelen op basis van deze risico's (obstakel 2);
- Dit kan uiteindelijk voortkomen uit een gebrek aan bewustzijn en kennis over de urgentie en impact van cyberdreigingen (obstakel 1).

Bedrijven binnen het mkb, **met name achterblijvers, zijn zich voornamelijk bewust van de interne obstakels** of zijn zich überhaupt niet bewust van de mogelijke obstakels.

Subvraag 2: Welke (publiek-private) mogelijkheden/ tools bestaan er om bedrijven in staat te stellen hun huidige eigen cyberweerbaarheidsniveau en hun optimaal cyberweerbaarheidsniveau te identificeren (bijvoorbeeld: metrieken, interventies, instrumentarium, classificaties van bedrijven en sectoren, etc.), en hoe goed werken die tools?
Antwoord subvraag 2: Er zijn **64 algemene hulpmiddelen** geïdentificeerd die bedrijven binnen het mkb kunnen gebruiken om hun cyberweerbaarheid te versterken; dit zijn gratis, publiekelijk beschikbare hulpmiddelen die relevant zijn voor specifiek het mkb, en geen vergevorderde kennis omtrent cyber vereisen. Elk hulpmiddel heeft een primair doel. Dit doel is voor elk van de 64 hulpmiddelen inzichtelijk gemaakt door ze onder te brengen in een van de acht geïdentificeerde obstakels. De vorm van elk hulpmiddel kan verschillen; zo zijn er bijvoorbeeld online informatiepagina's, interactieve bijeenkomsten, vragenlijsten inclusief adviezen, helpdeks, stappenplannen, etc.

Het overzicht aan algemene hulpmiddelen leidt tot de volgende twee overkoepelende conclusies:

- **De verdeling van het aanbod aan hulpmiddelen is uit balans.** De focus ligt voornamelijk op het creëren van handelingsperspectief gezien ongeveer driekwart van de hulpmiddelen is gericht op het aanbieden van maatregelen die het bedrijf kan nemen om hun cyberweerbaarheid te versterken. Hoewel dit belangrijk is, lijkt er relatief minder aandacht te zijn voor het creëren van cyberbewustzijn en -kennis, inzicht in risico's (binnen het bedrijf en in de waardeketen), afwegingen rondom investeringen, cyberrichtlijnen voor het mkb en de vindbaarheid van (overheids-)hulpmiddelen.
- **Er ontbreekt synergie in het aanbod aan hulpmiddelen.** Met 64 hulpmiddelen vanuit 35 publieke en private organisaties en samenwerkingsverbanden is het aanbod groot en divers, maar ook onoverzichtelijk en onsamenhangend.

Naast de 64 algemene hulpmiddelen, zijn er ook **187 hulpmiddelen geïdentificeerd vanuit 51 private samenwerkingsverbanden;** denk bijvoorbeeld aan brancheorganisaties. Deze hulpmiddelen zijn met name gericht op kennisdeling en voorlichting, het organiseren van bijeenkomsten, het aanbieden van cybertools en het delen van dreigingsinformatie. Vaak zijn deze hulpmiddelen alleen beschikbaar voor aangesloten leden.

Het **DTC ondersteunt deze samenwerkingsverbanden** en het aantal groeit elk jaar. Samenwerkingsverbanden, zoals bijvoorbeeld Cyberweerbaarheidscentrum Greenport, zijn een geschikt instrument voor het DTC om effectief hulp te bieden aan mkb bedrijven binnen specifieke sectoren. Gezien de behoefte vanuit het mkb voor meer verbinding en communicatie – zowel verticaal tussen verschillende lagen in het Nederlandse cyberlandschap en horizontaal tussen bedrijven onderling – lijken deze samenwerkingsverbanden goed gepositioneerd om hier een rol in te vervullen. Echter, er is meer onderzoek nodig naar de mogelijke regie- en coördinerende rol van de overheid met betrekking tot deze samenwerkingsverbanden. Het brede aanbod van hulpmiddelen vanuit de samenwerkingsbanden kan namelijk verwarrend zijn voor bedrijven binnen het mkb omdat onduidelijk is welke informatie te vinden is bij welke partij.

Dieper ingaand op hulpmiddelen die specifiek als doel hebben bedrijven te helpen hun huidige of optimale cyberweerbaarheidsniveau in kaart te brengen, zijn er vier metrieken uit de selectie van hulpmiddelen die zich hierop richten:

- Identificeren van het **huidige cyberweerbaarheidsniveau:**
  1. De CyberVeilig Check van het DTC;
  2. De Basisscan Cyberweerbaarheid van het DTC;
- Identificeren van het **optimale cyberweerbaarheidsniveau:**
  3. De Risicoklasse Tool van het DTC;
- Identificeren van het **huidige en optimale cyberweerbaarheidsniveau:**
  4. CYRA (CyberRating) van CW Brainport, FERM Rotterdam, MKB Cyber Campus ASML en TÜV Nord Nederland.

(1,2) De **CyberVeilig Check** en de **Basisscan Cyberweerbaarheid** zijn enkel gericht op het in kaart brengen van het huidige cyberweerbaarheidsniveau. Deze metrieken bieden geen inzicht in het optimale niveau en de stappen die een bedrijf moet nemen om tot dit optimale niveau te komen. Beide metrieken worden aangeboden in de vorm van een online vragenlijst over de geïmplementeerde cybermaatregelen bij een bedrijf. Op basis van de gegeven antwoorden wordt dan een aantal aanbevelingen gedaan die kunnen helpen in het versterken van de cyberweerbaarheid.

(3) De **Risicoklasse Tool** is enkel gericht op het in kaart brengen van het **optimale cyberweerbaarheidsniveau.** Het optimale niveau wordt wel bepaald aan de hand van een risicoklasse maar er wordt geen uitgebreide risicoanalyse uitgevoerd. Daarnaast biedt het geen inzicht in het huidige cyberweerbaarheidsniveau. De Risicoklasse Tool is eveneens een online vragenlijst, maar richt zich meer op variabelen die invloed hebben op het risicoprofiel van een bedrijf, zoals de grootte van de onderneming, het type data waarmee gewerkt wordt, de sector, etc. Op basis van de antwoorden wordt het bedrijf ingedeeld in een risicoklasse, met de daarbij horende beveiligingsmaatregelen die minimaal van toepassing zijn.

(4) De **CYRA** is zowel op het huidige als optimale cyberweerbaarheidsniveau gericht. Het optimale cyberweerbaarheidsniveau wordt vastgesteld aan de hand van een korte vragenlijst waarin het risicoprofiel wordt meegenomen. Dit is niet een uitgebreide risicoanalyse en het is aan het bedrijf zelf om te bepalen wat hun optimale cyberweerbaarheidsniveau is. Het huidige cyberweerbaarheidsniveau wordt vastgesteld aan de hand van een uitgebreide self-assessment. Verder biedt de CYRA als vervolgstap een (betaalde) audit aan. De CYRA is alleen toegankelijk voor bedrijven die lid zijn van samenwerkingsverbanden die aangesloten zijn bij de CYRA.

Hoe goed deze tools **werken is vooralsnog onbekend.** Inzicht in de effectiviteit van de drie metrieken vanuit het DTC is beperkt en voor de CYRA is dit binnen het onderzoek niet geëvalueerd. Voor alle vier de genoemde metrieken geldt dat ze **niet volledig aansluiten bij de behoefte van bedrijven binnen het mkb** om beter inzicht te krijgen in hun risico's en welke maatregelen ze zouden moeten nemen op basis van hun risicoprofiel.

Hoofdvraag 2

Hoofdvraag 2: Welke mogelijkheden zijn er voor de overheid om bedrijven te helpen om hun cyberweerbaarheidsniveau naar een voor hen optimaal niveau te brengen, met als resultaat dat bedrijven daadwerkelijk gebruik maken van deze mogelijkheden?

Subvraag 3: Welke beleidsmaatregelen werken wel en niet om bedrijven te stimuleren hun huidige en optimale cyberweerbaarheidsniveau in kaart te brengen?
Antwoord subvraag 3: In de context van dit onderzoek wordt het begrip 'beleidsmaatregel' breed opgevat, en geduid als acties die de overheid heeft ondernomen om bedrijven te stimuleren hun huidige en optimale cyberweerbaarheidsniveau in kaart te brengen. De tools vanuit het DTC, zoals genoemd bij subvraag 2, zijn belangrijke voorbeelden hiervan. Echter, de inspanningen van de overheid reiken verder. Kijkend naar **de publieke algemene hulpmiddelen,** richt de overheid zich onder andere op:

- Aanbieden van bewustwording programma's (Alert Online)
- Voorzien van informatie (Cybersecurity maatregelen DTC)
- Delen van kennis (DTC Community, Start Event 'Veilig online ondernemen' KVK)
- Delen van dreigingsinformatie (Waarschuwingsservice DTC)
- Opzetten van een meldpunt (Hackhelpdesk DTC, Nationale Politie)
- Hulp bij het interpreteren van cyberrichtlijnen (Webpagina NIS2 Digitale Overheid)
- Verbeteren van vindbaarheid van hulpmiddelen (Wegwijzer voor Cybersecurity Initiatieven DTC)

Aanvullende voorbeelden van deze beleidsmaatregelen staan genoemd in hoofdstuk '4. Overzicht huidige hulpmiddelen' in de vorm van algemene hulpmiddelen die aangeboden worden in het publieke domein (zie Tabel 4).

Echter geldt voor deze beleidsmaatregelen, dat het **lastig is te beoordelen welke wel en niet werken** binnen de scope van dit onderzoek. Dit heeft twee redenen:

- De geïnterviewde bedrijven binnen het mkb hebben **geen gebruik gemaakt van de hulpmiddelen.** Slechts 9% van de bedrijven gaf überhaupt aan bekend te zijn met het DTC en/of NCSC.
- Vanuit het DTC is er **geen concrete data beschikbaar** over de effectiviteit van de hulpmiddelen die ze aanbiedt. Dit geldt ook voor het NCSC en de KVK. Alle drie de partijen hebben wel inzicht in het gebruik en de waardering van de hulpmiddelen, maar kunnen niet aangeven in hoeverre een hulpmiddel effectief is, dus in hoeverre het bijdraagt aan het versterken van de cyberweerbaarheid van bedrijven binnen het mkb.

Er is **meer onderzoek nodig** naar de meest effectieve en structurele manieren (bijvoorbeeld via een sectorale aanpak in samenwerking met brancheverenigingen etc.) waarop de overheid bedrijven binnen het mkb kan stimuleren om hun huidige en optimale cyberweerbaarheidsniveau in kaart te brengen. Hiervoor is het belangrijk de effectiviteit van het huidige aanbod aan hulpmiddelen te evalueren, zodat deze beter kunnen aansluiten bij de behoefte van bedrijven binnen het mkb.

Subvraag 4: Hoe kunnen we stimuleren dat bedrijven weten hoe ze hun cyberweerbaarheid moeten versterken en dat ze vervolgens deze verbeteringen ook willen en kunnen doorvoeren?
Antwoord subvraag 4[136]***:*** Als resultaat van dit onderzoek zijn **9 strategische aanbevelingen gedaan** (zie Figuur 8) die de overheid richting geven in het verkleinen van de cyberweerbaarheidskloof in Nederland, door bedrijven binnen het mkb te helpen met het versterken van hun cyberweerbaarheid. Hiervoor is regie vanuit de overheid belangrijk, gezien het Nederlandse cyberlandschap een groot en breed scala aan publiek/private partijen bevat die ieder op hun eigen manier hulp bieden aan bedrijven binnen het mkb, maar waar de onderlinge synergie soms ontbreekt.

De 9 strategische aanbevelingen zijn onderverdeeld in **3 oplossingsrichtingen**, namelijk:

1. **Organiseer een gerichte, uniforme, structurele aanpak.** Deze oplossingsrichting richt zich op het netwerk van partijen in het cyberlandschap (zoals overheidsinstanties, branche-/belangenverenigingen, samenwerkingsverbanden en schakelorganisaties), en hun onderlinge verbinding. Vanuit deze partijen is namelijk een uniforme aanpak nodig, specifiek gericht op het mkb, en dit is naast een gedeelde visie alleen mogelijk met duidelijke rollen en verantwoordelijkheden, horizontale en verticale samenwerking en effectieve communicatie.
2. **Bied passende hulp aan het gehele mkb.** Met een uniforme aanpak en een sterke verbinding tussen partijen in het cyberlandschap kan vervolgens passende hulp worden geboden aan bedrijven binnen het mkb. Hierin is essentieel dat de hulp aansluit bij de behoefte van het mkb, wat alleen kan in samenwerking met het mkb.
3. **Stimuleer en zet aan tot handelen.** Een sterk netwerk en passende hulp zijn essentieel maar garanderen niet de daadwerkelijke versterking van de cyberweerbaarheid van het mkb. Deze oplossingsrichting richt zich daarom op het activeren van bedrijven zodat ze hun eigen verantwoordelijkheid inzien en op zich nemen.

De strategische aanbevelingen worden hieronder verder toegelicht.

Figuur 8 Strategische aanbevelingen, onderverdeeld in oplossingsrichtingen met als doel het verkleinen van de cyberweerbaarheidskloof in Nederland

[136] Bij de beantwoording van deze subvraag wordt met 'we' gerefereerd naar de overheid

Oplossingsrichting 1: Organiseer een gerichte, uniforme, structurele aanpak.

1. **Benadruk en bevorder de coördinerende en faciliterende regierol van het DTC/NCSC als (publiek-privaat) loket,** wegwijzer, kennisbank en bron van ondersteuning en advies, en vergroot haar bekendheid. Dit creëert overzicht in het cyberlandschap en maakt het voor de mkb'er makkelijker de hulp vanuit de overheid te vinden en, indien nodig, doorverwezen te worden naar de juiste partij. Voor inspiratie uit het buitenland zie het Verenigd Koninkrijk waar het NCSC een centrale rol inneemt en haar taken gekoppeld zijn aan de overkoepelende ambitie om als Verenigd Koninkrijk een van de meest veilige en aantrekkelijke digitale economieën te zijn om in te wonen, zaken te doen en te investeren.
2. **Verbind met het mkb door structurele samenwerking** met een ondersteunend netwerk van overheidsinstanties, branche-/belangenverenigingen, samenwerkingsverbanden en schakelorganisaties, waarbij verantwoordelijkheden duidelijk zijn belegd. Dit bevordert de informatiedeling en samenwerking (ook tussen overheidsinstanties), en maakt het bereiken van een groter deel van het mkb mogelijk. Door deze connecties te versterken kan ook het 'groot-helpt-klein' concept bevorderd worden waarbij meer volwassen bedrijven kleinere organisaties in de waardeketen helpen hun cyberweerbaarheid te versterken om zo afhankelijkheidsrisico's in de keten te mitigeren. Een voorbeeld uit het buitenland van een brede, publiek-private samenwerking is het Duitse samenwerkingsplatform 'Alliance for Cyber Security'.
3. **Communiceer en benadruk het belang en de urgentie van cyberweerbaarheid** door middel van uniforme informatievoorziening via betrouwbare, vindbare en herkenbare kanalen voor het mkb. Het ontbreken van cyberbewustzijn en -kennis is een fundamenteel obstakel en een waar het mkb een duidelijke rol ziet voor de overheid in de vorm van voorlichting over allerhande onderwerpen rondom cyberveiligheid.

Oplossingsrichting 2: Bied passende hulp aan het gehele mkb.

4. **Bouw voort op bestaande volwassenheidsmodellen en bied een toegankelijke en hanteerbare metriek/tool aan** voor het in kaart brengen van het huidige en optimale cyberweerbaarheidsniveau, op basis van een risicoanalyse. Een belangrijk obstakel voor bedrijven binnen het mkb is dat er weinig of geen zicht is op de interne risico's van de organisatie. De overheid kan hierbij helpen door het ontwikkelen van een metriek/tool die op basis van een risicoanalyse en het huidige cyberweerbaarheidsniveau concreet handelingsperspectief biedt om de cyberweerbaarheid te versterken tot een optimaal niveau. Voor inspiratie uit het buitenland zie bijvoorbeeld het Deense D-seal. Dit is een certificeringsprogramma voor IT-beveiliging en verantwoord gebruik van gegevens. Het is bedoeld om het beveiligingsniveau van een bedrijf te communiceren en zal vertrouwen creëren voor klanten en consumenten, en de digitale verantwoordelijkheid van bedrijven bevorderen.
5. **Bied een compact en uniform geheel aan hulpmiddelen aan,** die betrouwbaar en begrijpelijk zijn, aansluiten bij de behoefte van het mkb en waar nodig gedifferentieerd zijn naar een specifieke sector; evalueer periodiek de effectiviteit van de hulpmiddelen. Er wordt al veel hulp aangeboden, maar er ontbreekt samenhang en synergie. Bij het samenvoegen, verbeteren of ontwikkelen van hulpmiddelen dient het hulpmiddel te voldoen aan de volgende negen kenmerken:
   - Adresseert een concreet obstakel
   - Sluit aan bij een breed gedragen behoefte van bedrijven binnen het mkb
   - Is ontwikkeld in samenwerking met het mkb én publieke/private partners
   - Biedt tijdig, een betrouwbaar en begrijpelijk en realistisch handelingsperspectief
   - Is uniform en gestandaardiseerd voor type hulpmiddelen die algemeen toepasbaar zijn voor het gehele mkb, zoals een online lijstje cyber basismaatregelen
   - Staat, waar relevant, in proportionele verhouding met het risicoprofiel van een bedrijf binnen het mkb
   - Is vertaald, waar mogelijk, naar een subgroep van het mkb, zoals een sector of branche
   - Ondersteunt bedrijven in het naleven van regelgeving binnen een duidelijk, uitgewerkt wettelijk kader met heldere, toegespitste richtlijnen
   - Wordt periodiek geëvalueerd op actualiteit, gebruik en effectiviteit, en verbeterd op basis van feedback vanuit het mkb

   Een voorbeeld uit het buitenland waar informatie en hulpmiddelen duidelijk en overzichtelijk aangeboden worden, en waar nodig vertaald naar een specifieke doelgroep of sector, is het NCSC van het Verenigd Koninkrijk.
6. **Help bedrijven met het aantonen van hun cyberweerbaarheid door middel van een cyberveiligheidsbewijs,** het selecteren van de juiste ICT-dienstverlener via een **ICT-keurmerk, en het samenwerken met leveranciers (SLA's).** Bedrijven binnen het mkb zijn vaak overgeleverd aan hun ICT-leverancier zonder garantie van proportionele, kwalitatieve en transparante dienstverlening. Ze hebben behoefte aan ondersteuning in het selecteren van een geschikte ICT-leverancier via een ICT-keurmerk (zie bijvoorbeeld het Deense D-seal of het Franse ExpertCyber), het investeren in de juiste cyberweerbaarheidsmaatregelen en het opstellen van onderlinge afspraken. Het cyberveiligheidsbewijs is een breed, begrijpelijk en toegankelijk middel voor bedrijven om klanten en leveranciers te garanderen dat bepaalde cyberweerbaarheidsmaatregelen geïmplementeerd zijn. Dit is bijvoorbeeld interessant voor bedrijven die digitale producten en diensten aanbieden, maar te klein zijn voor een ISO27001 certificering. Voor inspiratie uit het buitenland kan eventueel gekeken worden naar Cyber Essentials uit het Verenigd Koninkrijk.

Oplossingsrichting 3: Stimuleer en zet aan tot handelen.

7. **Help bedrijven bij het investeren in cyberweerbaarheids-maatregelen** die passen bij het risicoprofiel, de middelen en capaciteit van het bedrijf; bied subsidies aan waar nodig. “Wanneer is goed, goed genoeg?”, dat is de vraag voor veel bedrijven binnen het mkb als het gaat om het investeren in cyberweerbaarheidsmaatregelen. Er is behoefte aan ondersteuning op dit vlak gezien het mkb vaak niet de kennis of de tijd heeft om een weloverwogen en passende keuze te maken omtrent de “kosten-baten balans” van cyberweerbaarheidsmaatregelen.
8. **Stel duidelijke wettelijke kaders en richtlijnen,** assisteer bedrijven in het succesvol implementeren van wetgeving en houd toezicht en handhaaf op het correct naleven ervan. Bedrijven binnen het mkb hebben soms geen duidelijk zicht op de standaarden waar ze aan moeten voldoen als het gaat om cyberveiligheid, zeker nog niet rondom de nieuwe NIS2-wetgeving. Voorlichting over dit onderwerp en duidelijke, concrete, toegespitste richtlijnen zijn nodig voor succesvolle en breed gedragen implementatie.
9. **Onderzoek of er voor bedrijven die niet onder NIS2 vallen aanvullende stimulerende maatregelen nodig zijn** om het mogelijk te maken het gehele mkb naar hoger cyberweerbaarheidsniveau te tillen. NIS2 zal een grote impact hebben op bedrijven die onder deze nieuwe wetgeving vallen. De impact zal ook doorwerken in bedrijven die niet direct onder NIS2 vallen, maar wel in de waardeketen zitten met bedrijven voor wie dit wel geldt. Gezien het belang van een cyberweerbaar mkb over de gehele linie, is het essentieel dat bedrijven die niet onder NIS2 vallen en niet via hun waardeketen hiermee in aanraking komen, ook een bepaalde (minimale) cyberweerbaarheid hebben.

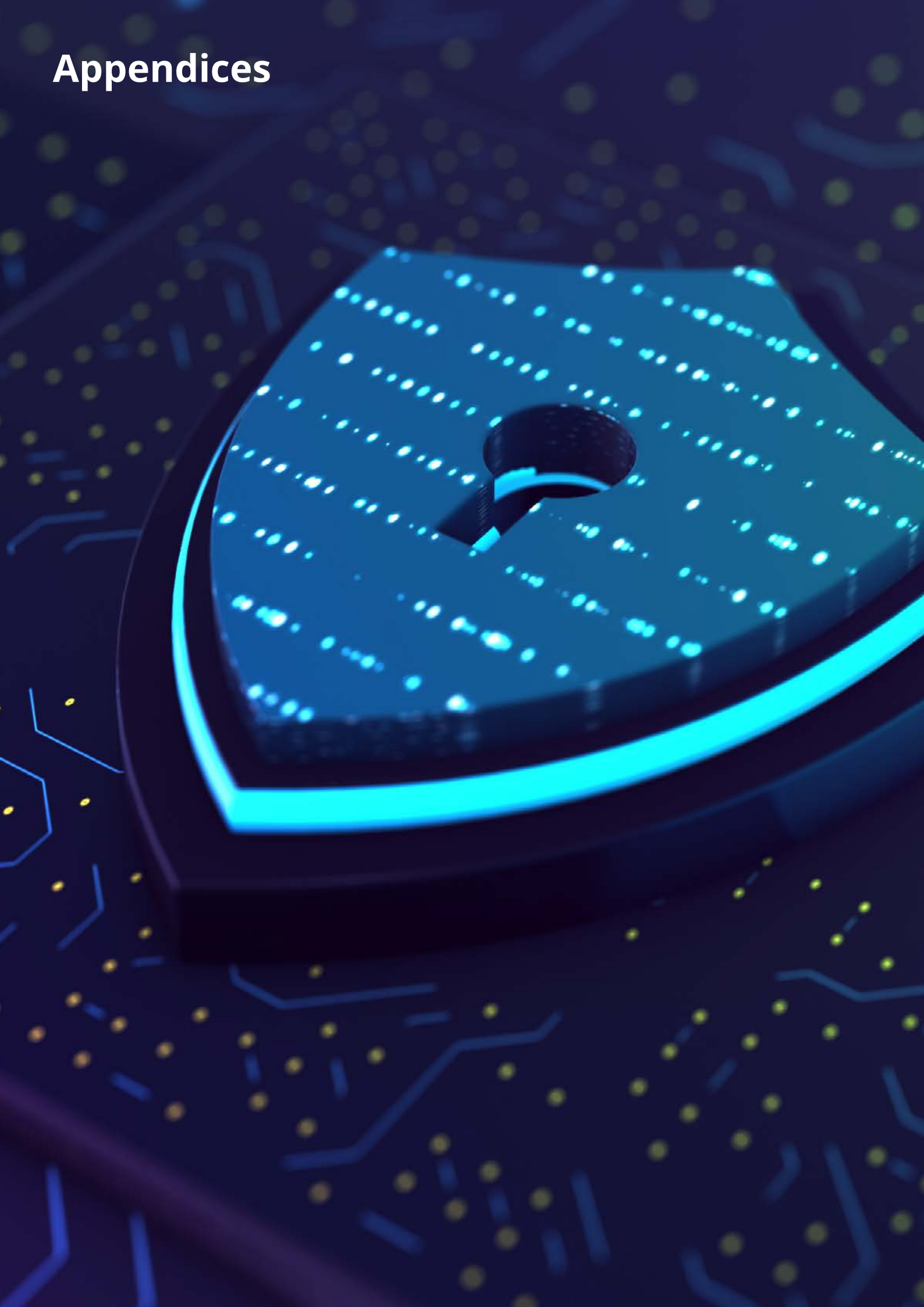
8. Literatuurlijst

[1] Voor meer informatie zie https://www.cybersecurityraad.nl/
[2] Cybersecuritybeeld Nederland 2021 & 2022, Nationaal Coördinator Terrorismebestrijding en Veiligheid
[3] "Veel kleine bedrijven zijn onvoldoende cyberweerbaar", Digital Trust Center webpagina, 22 mei 2023
[4] Cybersecuritymonitor 2022, Centraal Bureau voor de Statistiek
[5] Digital Trust Center, organisatie opgericht in 2018 door het ministerie van Economische Zaken en Klimaat ter ondersteuning van Nederlandse bedrijven in veilig digitaal ondernemen
[6] Nationaal Cyber Security Centrum, onderdeel van het ministerie van Justitie en Veiligheid en verantwoordelijk voor het bevorderen van de digitale veiligheid in Nederland
[7] Zie "Afspraken maken met een IT-leverancier" van het Digital Trust Center
[8] Zie "Minister wil cybersecurity-keurmerk om mkb te helpen" van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), 2 oktober 2023
[9] Nederlandse Cybersecuritystrategie 2022–2028, Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022)
[10] Cyberbeveiliging: EU-aanpak van cyber¬dreigingen, Europese Raad (2023)
[11] Cybersecurity Woordenboek, CyberVeilig Nederland
[12] Rapport Digitale weerbaarheid zzp en mkb, Digital Trust Center (DTC) Benchmark onderzoek (2023)
[13] Cybersecuritybeeld Nederland 2022, Nationaal Coördinator Terrorismebestrijding en Veiligheid (2022)
[14] Bij de beantwoording van deze subvraag wordt met 'we' gerefereerd naar de overheid
[15] De samenstelling van de klankbordgroep staat vermeld in Appendix A – Leden van de klankbordgroep
[16] De namen van de 32 geïnterviewde bedrijven zijn geanonimiseerd
[17] Zie Appendix C – Begrippenlijst voor de definitie van het begrip 'hulpmiddelen'
[18] Het Nederlandse midden- en kleinbedrijf Europees vergeleken, Centraal Bureau voor de Statistiek (2021)
[19] Zie KVK.nl, 'Data over de bedrijvendynamiek – 2023 1e kwartaal'
[20] Cybersecurity Woordenboek, Cyberveilig Nederland
[21] Zie tools.digitaltrustcenter.nl/cyberveilig-check/
[22] Zie cbs.nl, Cybersecuritymonitor 2022
[23] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
[24] Stappenplan risicoanalyse, Digital Trust Center
[25] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[26] Cybersecuritybeeld Nederland 2023, Nationaal Coördinator Terrorismebestrijding en Veiligheid, (2022)
[27] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[28] The Law and Economics of Cyber Security, B.F.H. Nieuwesteeg (2018)
[29] Benchmark Onderzoek, Digital trust Center (2023)
[30] Cyber Security Monitor 2022, Centraal Bureau voor de Statistiek (2023)
[31] De variabelen zijn in afstemming met de klankbordgroep geïdentificeerd
[32] Het Nederlandse midden- en kleinbedrijf Europees vergeleken, Centraal Bureau voor de Statistiek (2021)
[33] Cyber Security Monitor 2022, Centraal Bureau voor de Statistiek (2023)
[34] Zie brief regering 'Stand van zaken implementatie NIS2 en CER richtlijnen', Tweede Kamer der Staten-Generaal, 31 januari 2024
[35] Cyber Security Monitor 2022, Centraal Bureau voor de Statistiek (2023)
[36] Informatie verkregen vanuit de klankbordgroep tijdens de starbijeenkomst op 18-08-2023
[37] Nederlandse Cybersecuritystrategie 2022-2028, Rijksoverheid (2022)
[38] Adviesrapport 'Integrale aanpak cyberweerbaarheid', Cyber Security Raad (2021)
[39] Zie digitaltrustcenter.nl
[40] Meer mogelijk NCSC om dreigings- en incidentinformatie te delen, Nationaal Cyber Security Centrum (2022)
[41] Zie vraaghetdepolitie.nl, 'Wat doet de politie tegen cybercrime?'
[42] Cyber Security Monitor 2022, Centraal Bureau voor de Statistiek (2023)
[43] Informatie verkregen vanuit de klankbordgroep tijdens de starbijeenkomst op 18-08-2023
[44] Cybersecurity Woordenboek, Digital Trust Center (2023)
[45] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[46] CEOs' information security behavior in SMEs: does ownership matter?, Barlette et al. (2017)
[47] Risk and the Small-Scale Cyber Security Decision Making Dialogue - an UK Case Study, Osborn & Simpson (2018)
[48] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[49] Nederlandse Cybersecuritystrategie 2022-2028, Rijksoverheid (2022)
[50] Aanpak preventie cybercrime bij MKB, MKB-Nederland (2022)
[51] Aan de slag met het kwantificeren van cyberrisico's, Nationaal Cyber Security Centrum (2020)
[52] Kwantificering van cyberrisico's, Nationaal Cyber Security Centrum (2020)
[53] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[54] Cyberweerbaarheidsonderzoek MKB Brabant 2022, ACA IT-Solutions (2022)
[55] Risk and the Small-Scale Cyber Security Decision Making Dialogue - an UK Case Study, Osborn & Simpson (2018)
[56] Cyber Value at Risk in the Netherlands, Deloitte (2017)
[57] Op weg naar een lokale aanpak voor digitale weerbaarheid bij het midden- en kleinbedrijf, Middelman (2022)
[58] Cyber Value at Risk in the Netherlands, Deloitte (2017).
[59] Informatie verkregen vanuit de klankbordgroep (2023)
[60] "Nederlandse Cybersecuritystrategie (NLCS) 2022-2028: Ambities en acties voor een digitaal veilige samenleving", (2022)

[61] De zoektocht naar ICT-personeel in een krappe arbeidsmarkt, Van Hout (2020)
[62] Digitale Ethiek en veiligheid - Cybersecurity & Privacy - NEN
[63] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[64] https://www.encyclo.nl/begrip/ketenpartners
[65] Strategic Roadmap to building a World Class software engineering Organization, Gartner (z.d.)
[66] PrivacyWaakhond: Veel meer datalekken door cyberaanvallen gemeld, Wilman (2022)
[67] Informatie-uitwisseling landelijk dekkend stelsel, Brennenraedts et al. (2020)
[68] Informatie verkregen vanuit de klankbordgroep (2023)
[69] Nationaal Cyber Security Centrum (2023)
[70] Informatie verkregen vanuit de klankbordgroep (2023)
[71] Het NCSC en dreigingsinformatie, Nationaal Cyber Security Centrum (2021)
[72] Cybersecurity for SMEs - Challenges and Recommendations, ENISA (2021)
[73] Informatie verkregen vanuit de klankbordgroep (2023)
[74] Overzicht van samenwerkingsverbanden, DTC
[75] HU gaat cybersecurity toepasbaar maken voor kleinere bedrijven en organisaties, Hogeschool Utrecht (2023)
[76] CISO Circle of Trust, https://www.digitaltrustcenter.nl/samenwerkingsverband/ciso-circle-of-trust
[77] Stichting NL CISO Circle of Trust ontvangt OKTT-status, https://www.banken.nl/nieuws/24811/stichting-nl-ciso-circle-of-trust-ontvangt-oktt-status
[78] Voor meer informatie over de CCoT zie ook de nota 'CISO Circle of Trust' aangedragen aan de Cyber Security Raad over verschillende strategische thema's aan het verkleinen van de cyberweerbaarheidskloof door middel van publiek-private samenwerking
[79] Landelijk Dekkend Stelsel, NCTV https://www.nctv.nl/onderwerpen/landelijk-dekkend-stelsel
[80] Landelijk Dekkend Stelsel, NCSC https://www.ncsc.nl/onderwerpen/samenwerkingspartner-worden/aansluiting-op-het-landelijk-dekkend-stelsel-lds
[81] DTC deelt informatie over cyberdreigingen met bedrijfsleven, https://www.digitaltrustcenter.nl/dreigingsinformatie-ontvangen
[82] Zie tools.digitaltrustcenter.nl, 'CyberVeilig Check voor ZZP en MKB'
[83] Zie rijksoverheid.nl, 'Deelrapport Cybersecurity onderzoek Alert Online 2023 – bedrijfsleven', 29 sep 2023
[84] Cyberbeveiligingsbedrijf dat onderdeel is van de klankbordgroep voor dit onderzoek
[85] VWS is uiteindelijk niet meegenomen in de evaluatie in 5.4.7 gezien het hulpmiddel OpenKAT niet relevant is voor bedrijven binnen het mkb omdat het een relatief hoog kennisniveau vereist
[86] Zie appendix I voor het volledige overzicht
[87] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
[88] Zie DTC.nl, 'Subsidieregeling Cyberweerbaarheid stimuleert samenwerkingsverbanden'
[89] Zie DTC.nl, 'Overzicht van samenwerkingsverbanden'; de website vermeldt dat er 54/56 samenwerkingsverbanden zijn, echter bevat de volledige lijst zonder dubbelingen 58 samenwerkingsverbanden
[90] Zie cwgreenport.nl
[91] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
[92] Zie bsi.bund.de, 'Alliance for Cyber Security'
[93] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
[94] Op basis van de interviews is niet te achterhalen welke van deze hulpmiddelen het meest worden gebruikt of het beste werken
[95] Welke maatregelen specifiek meegenomen dienen te worden zal duidelijk moeten worden uit een vervolgonderzoek
[96] Zie ncsc.gov.uk, 'Verify suppliers'
[97] Zie cybermalveillance.gouv.fr, 'The professionals listed'
[98] Zie d-seal.eu
[99] 'DTC introduceert cybersubsidie voor kleine bedrijven', DTC, 27 oktober 2023
[100] NLdigital: 'Tweede Kamer dreigt digitale geletterdheid alsnog weg te bezuinigen', 26 mei 2023
[101] NLdigital: 'Nieuwkomers BBB en Volt hebben sterkste programma op gebied van digitalisering', 9 nov 2023
[102] Zie Curriculum.nu
[103] Kennisnet.nl: 'Expertisepunt digitale geletterdheid in het najaar gelanceerd', 25 september 2023
[104] Hoewel geen van de geïnterviewde bedrijven binnen het mkb aangaf bekend te zijn met NIS2, zal deze wetgeving de regels voor bedrijven die eronder vallen wel degelijk aanscherpen
[105] Zie www.autoriteitpersoonsgegevens.nl 'AVG voor ondernemers'
[106] Zie ncsc.gov.uk, 'Small & medium sized organisations – Support for sectors'
[107] Zie agconnect.nl, 'Kabinet komt dit jaar nog met subsidie cyberkeurmerk ict-leveranciers', 20 sep 2023
[108] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
[109] Zie d-seal.eu
[110] Zie danishbusinessauthority.dk
[111] Zie cybermalveillance.gouv.fr, 'ExpertCyber label'
[112] Zie ncsc.gov.uk, 'Verify suppliers'
[113] Zie ncsc.gov.uk, 'Cyber Essentials'
[114] Zie cbs.nl, ICT-kenmerken bij DTC-bedrijven, 2019-2023
[115] Zie ncsc.nl
[116] Zie sikkerdigital.dk/cyberhotline
[117] Zie cert.ssi.gouv.fr, 'About CERT-FR'
[118] Zie cybermalveillance.gouv.fr
[119] Zie NCSC.nl, 'Nationale cybersecurity organisaties gaan krachten bundelen', 7 september 2022
[120] Zie NCSC.gov.uk, 'What we do'
[121] HM Government, 'Government Cyber Security Strategy 2022-2030'
[122] Zie cyber.gouv.fr, 'About ANSSI'
[123] Zie NCSC.nl, 'Nationale cybersecurity organisaties gaan krachten bundelen', 7 september 2022
[124] Zie DTC.nl, 'Kabinetsstrategie Digitale Economie: versterk cybersecurity', 26 oktober 2023

[125] Zie ncsc.nl, 'Basismaatregelen cybersecurity'
[126] Zie digitaltrustcenter.nl, 'Starten met cybersecurity? Begin met deze maatregelen'
[127] Zie kvk.nl, 'Werk jij digitaal veilig? Controleer het met de checklist'
[128] Definitie bepaald op basis van afstemming met CSR
[129] Analyse volwassenheidsmodellen voor informatiebeveiliging, Informatiebeveiliging Magazine – De Haagse Hogeschool
[130] Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for Nist Cyber Security Framework. Computer Science & Information Technology (CS&IT), 7(3), 51-62
[131] https://cyberveilignederland.nl/woordenboek
[132] Stappenplan risicoanalyse, Digital Trust Center
[133] Analyse volwassenheidsmodellen voor informatiebeveiliging, Informatiebeveiliging Magazine – De Haagse Hogeschool
[134] Information Security Management Maturity Models (2022). Procedia Computer Science. Volume 213, 49-57
[135] Zie cyberrating.nl
[136] Bij de beantwoording van deze subvraag wordt met 'we' gerefereerd naar de overheid

Appendices



Appendix A – Leden van de klankbord-groep

Naam	Organisatie
Irene van der Zanden	DTC
Jasper Tiemann	NetW
Nelly Ghaoui	EZK
Nicole Mallens	VNO-NCW en MKB Nederland
Peter Franssen	Eye Security
David Kortleven	Plate
Pieter Versloot	Plate
Mai Elmar	MPI
Matty van den Berg	Watertalent

Tabel 9 Leden van de klankbordgroep.

Appendix B – Overzicht Sectoren

Tabel 10 toont de sectoren waarnaar de bedrijven binnen het mkb die deel hebben genomen aan het onderzoek ingedeeld zullen worden. De lijst is overgenomen van de KVK die deze SBI-codes (Standaard Bedrijfsindeling) aanhoudt. De laatste twee codes (T: Huishoudens als werkgever; niet-gedifferentieerde productie van goederen en diensten door huishoudens voor eigen gebruik) en (U: Extraterritoriale organisaties en lichamen) zijn weggehaald omdat ze niet relevant zijn voor dit onderzoek.

Sectoren binnen het mkb zoals gebruikt voor dit onderzoek (SBI-codes KVK)
A. Landbouw, bosbouw en visserij
B. Winning van delfstoffen
C. Industrie
D. Productie en distributie van en handel in elektriciteit, aardgas, stoom en gekoelde lucht
E. Winning en distributie van water; afval- en afvalwaterbeheer en sanering
F. Bouwnijverheid
G. Groot- en detailhandel; reparatie van auto's
H. Vervoer en opslag
I. Logies-, maaltijd- en drankverstrekking
J. Informatie en communicatie
K. Financiële instellingen
L. Verhuur van en handel in onroerend goed
M. Advisering, onderzoek en overige specialistische zakelijke dienstverlening
N. Verhuur van roerende goederen en overige zakelijke dienstverlening
O. Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen
P. Onderwijs
Q. Gezondheids- en welzijnszorg
R. Cultuur, sport en recreatie
S. Overige dienstverlening

Tabel 10 Overzicht sectoren zoals gedefinieerd door de KVK.

Appendix C – Begrippenlijst

Begrip	Definitie
Attack surface (aanvals-oppervlak)	Alle punten waar een organisatie kwetsbaar kan zijn voor potentiële aanvallen.
Cyberbewustzijn	In hoeverre individuen of organisaties bewust zijn van de cyberrisico's in hun omgeving.
Cyberveiligheid	Cyberveiligheid omvat alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer.
Cybervolwassenheid	Het niveau van bekwaamheid van een organisatie met betrekking tot cyberveiligheid.
Cyberweerbaarheid	Het vermogen van een bedrijf om (relevante) digitale risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken.
Cyberweerbaarheidskloof	Het verschil tussen voorlopers en achterblijvers aangaande cyberweerbaarheid in het mkb.
Dreigingslandschap	De actuele en potentiële bedreigingen en risico's die van invloed zijn op de cyberbeveiliging van een systeem, organisatie of netwerk.
Exploiteren	Het gebruikmaken van kwetsbaarheden in systemen.
Handelingsperspectief	Mogelijke acties of benaderingen die kunnen worden gevolgd om een doel te bereiken of een probleem op te lossen, of in dat geval, een obstakel te overwinnen.
Hulpmiddelen	Alle niet-commerciële middelen die bedrijven binnen het mkb in Nederland kunnen helpen hun cyberweerbaarheid te versterken.
Klankbordgroep	Een groep mkb'ers die worden geraadpleegd voor advies en feedback over specifieke kwesties.
Obstakels	Barrières of problemen die mkb'ers in de weg staan bij het versterken van hun cyberweerbaarheidsniveau.
Richtlijnen	Aanbevelingen of voorschriften die dienen als leidraad voor het uitvoeren van bepaalde taken of het nemen van beslissingen.
Schaalvoordelen	Financiële voordelen die ontstaan naarmate de afname toeneemt.
Subcommissie	Een kleinere commissie binnen een organisatie of commissie, belast met specifieke taken of verantwoordelijkheden binnen een domein.

Tabel 11 Begrippenlijst.

Appendix D – Overzicht samenwerkings-verbanden

Samenwerkingsverband	Kennis-deling	Bijeen-komst	Cyber-tools	Dreigings-info	Advies	Campag-ne	Certifi-caten	Crisis-oefening	Meld-punt	Data-base	Verzeke-ring	Totaal
Adfiz	3	1	2		1							7
Agrifood Cyberweerbaarheid	1	1	1									3
Bouwend Nederland	3	1										4
CCRC	1				1			1				3
CIO Platform Nederland		1		1			1	1				4
CISO Circle of Trust (CCoT)	1			1								2
Connect2trust	2	1										3
Cyber Netwerk Drechtsteden	3	1	3									7
Cyber Security Programma Noordzeekanaalgebied		1	1	1					1			4
Cyber Weerbaarheidscentrum Brainport	2	3		1	1							7
Cyberchain	1									1		2
Cybernetwerk Zuid-Hollandse Eilanden	1	2	1									4
Cybersecurity Centrum voor de Maakindustrie	1	1	1									3
CyberVeilig Westfriesland	1	2	1		1							5
Cyberweerbaarheid in Limburg		1										1
Cyberweerbaarheidscentrum Greenport	1	3	1	1	1							7
Cyberweerbaarheidsplan DIVD				1								1
CYRA	1						1					2
CYSSEC (Cybersecurity Synergie Schiphol Ecosysteem)	1	2	1	1								5
Dutch Cybersecurity Assembly (DCA)	1	2										3
Federatie van technologiebranches (FHI)	1	1										2
FERM		2	1	2	1			1	1			8
GEU	3		1									4
Hi Delta	1	2	1									4
i-CERT				1								1
INretail	3											3
Kennisgroep Cyber Security			1									1
Koninklijke Horeca Nederland	1											1
MDMX	2	1	1		1							5
MKB Cyber Campus	4	1					1		1			7
MKB Cyber Heroes (HackShield for Grown-ups)		3				3						6
MKB Cybersecurity Governance scan	1		1									2
Nationale Beheersorganisatie Internet Providers (NBIP)			1	1								2
Netwerk voor Risk-Based Cyberweerbaarheid	3			1	1						1	6
NIDV Cyberweerbaarheid DVI	1	2								1		4
Noord Holland Samen Veilig	1	1				2						4
NRTO	2	1										3
Pensioenfederatie	3			1								4
Platform Zelfstandige Ondernemers (PZO)		1	2									3
Samenwerking Noord	1	3	1									5
Smart Industry / FME	1	1	1					1				4
SRA	2	1										3
Stichting Cyber Safety Noord Nederland		3										3
Synthesis		2										2
TechSoup Nederland	2	1	1									4
Thuiswinkel.org	1		1				1					3
Transport en Logistiek Nederland	2	1										3
Vergroting cyberweerbaarheid groentezaadveredelingsbedrijven	1			1								2
Verhogen cyberweerbaarheid Beveiligingsinstallaties	3	1	1									5
Vitaal Digitaal Breda		1										1
Z-CERT	1	1		2	1							5
Totaal	**64**	**53**	**26**	**16**	**9**	**5**	**4**	**4**	**3**	**2**	**1**	**187**

Tabel 12 Overzicht samenwerkingsverbanden en aanbod aan hulpmiddelen.

Appendix E – Overzicht interviews

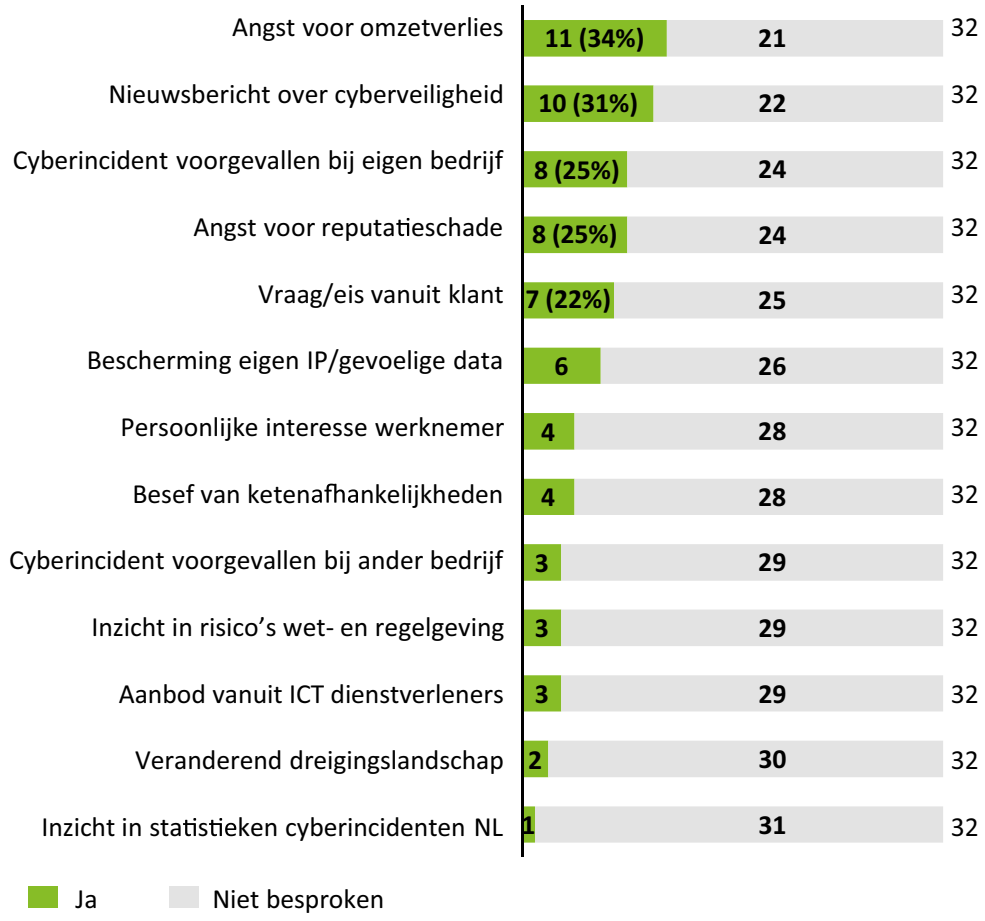
#	Partij	Publiek	Privaat
1	Centrum Informatiebeveiliging en Privacybescherming (CIP)		●
2	Digital Trust Center (DTC)	●	
3	Eye Security		●
4	Ministerie van Economische Zaken en Klimaat (EZK)	●	
5	ING		●
6	Ministerie van Volksgezondheid, Welzijn en Sport (VWS)	●	
7	Nationaal Cyber Security Centrum (NCSC, schriftelijk contact)	●	
8	Kamer van Koophandel (KVK, schriftelijk contact)	●	
9	Nationale Politie	●	
10	NLdigital		●
11	Security Delta (HSD)		●
12	Vereniging van Nederlandse Gemeenten (VNG)		●
13	Deloitte Denemarken		●
14	Deloitte Duitsland		●
15	Deloitte Engeland		●
16	Deloitte Frankrijk		●
17	Gemeente		●
18-49	Bedrijven binnen het mkb		●

Tabel 13 Overzicht van geïnterviewde partijen.

Appendix F – Interviewdata

Triggers

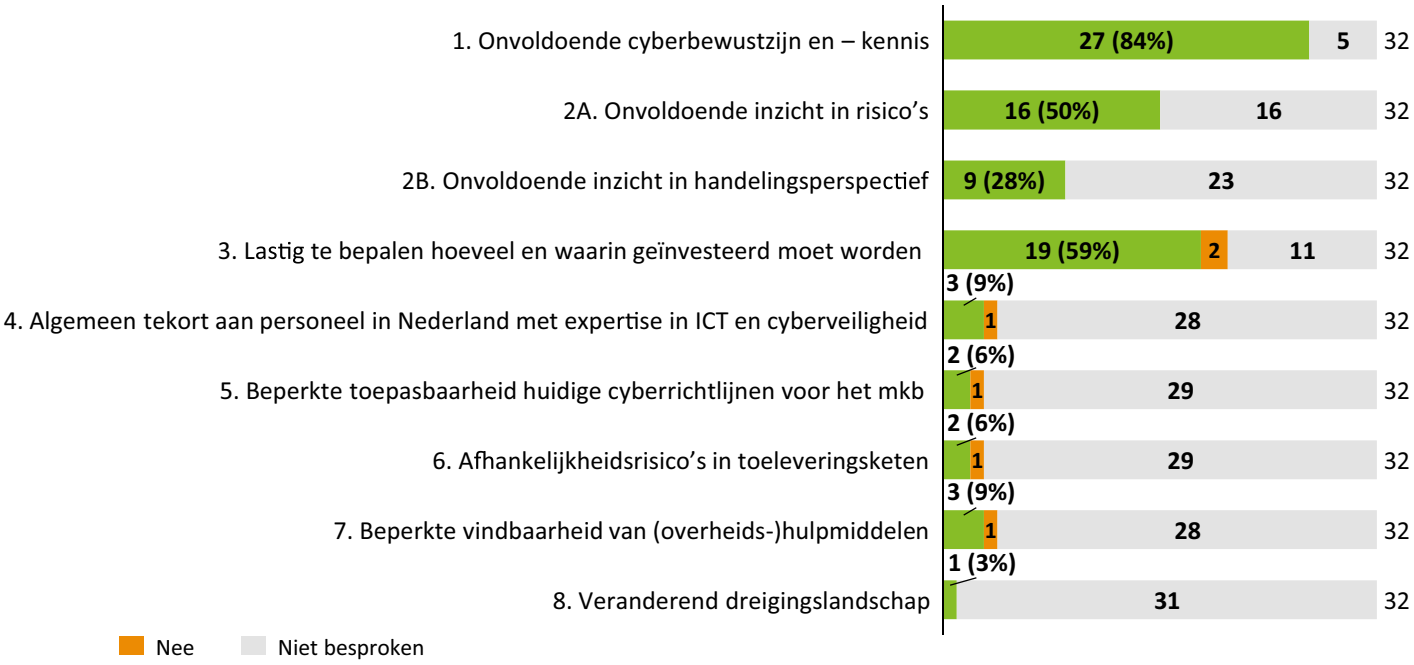
Figuur 9 toont de 'triggers' die geïnterviewden noemen als aanleiding voor het ondernemen van stappen richting een sterkere cyberweerbaarheid.



Figuur 9 Aanleidingen voor het versterken van de cyberweerbaarheid.

Obstakels

Figuur 10 toont de 8 obstakels en het aantal geïnterviewden dat aangeeft dat een obstakel voor hen een probleem is in het versterken van de cyberweerbaarheid.



Figuur 10 Het aantal keer dat obstakels genoemd worden tijdens de interviews.

Tabel 14 toont hoe vaak de 8 obstakels samen genoemd worden. De diagonale rij toont het totaal aantal keer dat een obstakel genoemd wordt en komt dus overeen met het aantal 'Ja' in Figuur 10.

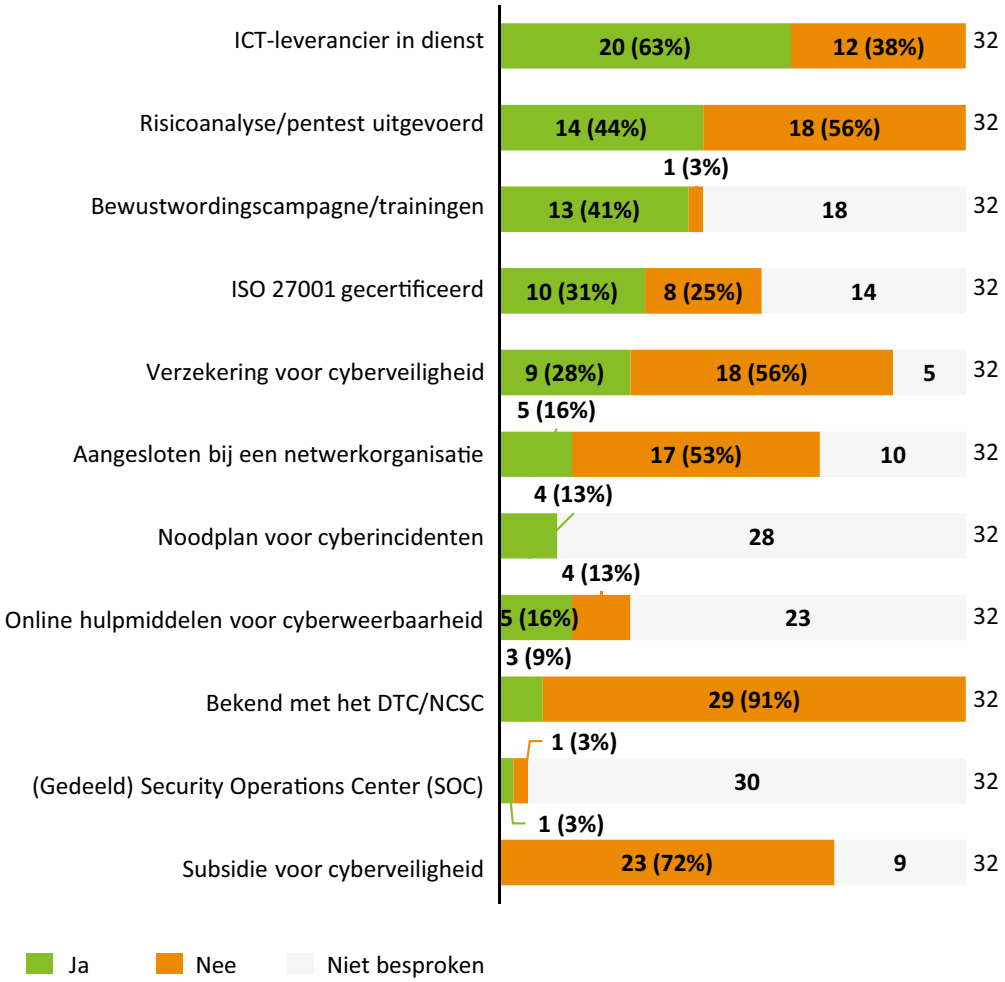
Om een voorbeeld te geven: obstakel 1 wordt in totaal 27 keer genoemd door de 32 geïnterviewden; in 15 van de 27 gevallen noemt de geïnterviewde ook obstakel 2A.

			Obstakel								
		Obstakel	1	2A	2B	3	4	5	6	7	8
Intern	1	Onvoldoende cyberbewustzijn en –kennis	27	15	7	17	3	1	2	3	1
	2	Onvoldoende inzicht in risico's	15	16	6	12	1	0	2	1	1
		Onvoldoende inzicht in handelingsperspectief	7	6	9	5	0	0	0	2	1
	3	Lastig te bepalen hoeveel en waarin geïnvesteerd moet worden	17	12	5	19	1	2	2	2	0
Extern	4	Algemeen tekort aan personeel in Nederland met expertise in ICT en cyberveiligheid	3	1	0	1	3	0	0	0	0
	5	Beperkte toepasbaarheid huidige cyberrichtlijnen voor het mkb	1	0	0	2	0	2	0	1	0
	6	Afhankelijkheidsrisico's in toeleveringsketen	2	2	0	2	0	0	2	0	0
	7	Beperkte vindbaarheid van (overheids-)hulpmiddelen	3	1	2	2	0	1	0	3	0
	8	Veranderend dreigingslandschap	1	1	1	0	0	0	0	0	1

Tabel 14 Aantal keer dat obstakels samen genoemd worden.

Typen hulpmiddelen die worden gebruikt

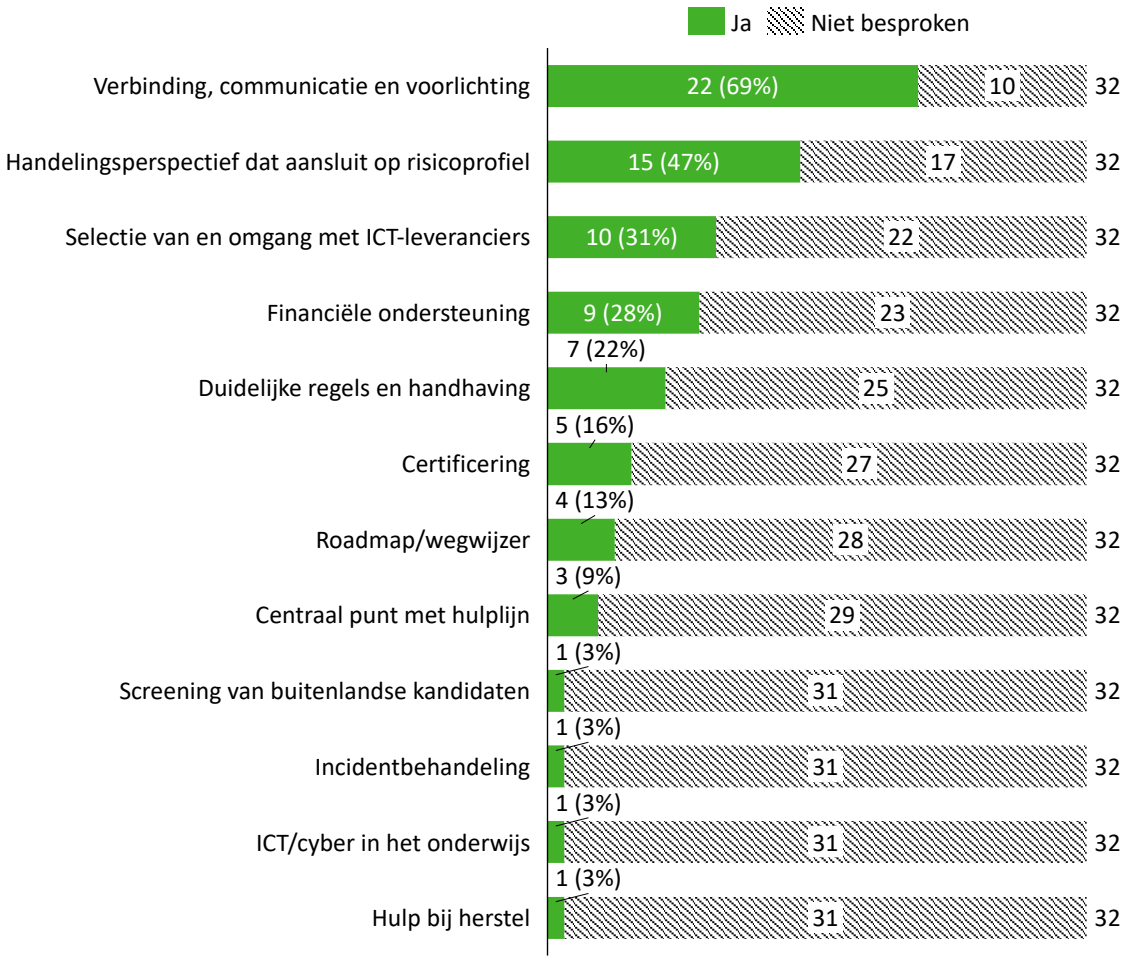
Figuur 11 toont het type hulp die geïnterviewden gebruiken, of niet gebruiken. Deze categorieën zijn anders dan de categorieën zoals weergegeven in Tabel 4 en Tabel 5 omdat geïnterviewden niet op dat detailniveau konden aangeven welke exacte hulpmiddelen ze gebruiken; dit ook vanwege het feit dat ze überhaupt weinig online hulpmiddelen gebruiken.



Figuur 11 Typen hulpmiddelen die worden gebruikt

Behoeftes

Figuur 12 toont de 12 behoeftes die geïnterviewden hebben geuit, en het totaal aantal keer dat ze zijn genoemd. Deze 12 categorieën zijn samengesteld door vergelijkbare behoeftes te bundelen in één categorie.
Tabel 15 toont weer de 12 behoeftes met een uitwerking van de inhoud, op basis van de interviews.



Figuur 12 Behoeftes van geïnterviewden.

#	Ja	Behoefte
1	22	**Verbinding, communicatie en voorlichting** Geïnterviewden geven aan een behoefte te hebben aan: • Een sterkere verbinding met de relevante partijen om in gesprek te gaan en samen te werken aan cyberveiligheid. Horizontaal gaat dit om bijvoorbeeld verbinding met (lokale) mede-mkb'ers en dienstverleners, en verticaal om de verbinding met brancheverenigingen, gemeente/provincie en de landelijke overheid. Een duidelijke rol voor de overheid is hier het faciliteren en stimuleren van deze verbindingen. • Met die verbinding is er vervolgens behoefte aan concrete, toegankelijke en doelgerichte communicatie, tussen de relevante partijen en bedrijven binnen het mkb. Onderling het gesprek aangaan creëert bewustzijn over het belang en de urgentie van cyberveiligheid, de impact van cyberincidenten en de rol/verwachtingen van de betrokken partijen. Hierbij is het belangrijk dat de overheid open en transparant is over haar eigen rol en volwassenheidsniveau, om zo ook een goed voorbeeld te geven. Belangrijk is dat de communicatie verloopt via betrouwbare kanalen waar bedrijven binnen het mkb bekend mee zijn, of bekend mee kunnen worden omdat ze er niet omheen kunnen; denk bijvoorbeeld aan de KVK of de accountant waar ze toch al vaste contactmomenten mee hebben. Verder is er behoefte aan meer directe communicatie, zoals bijvoorbeeld via een brief of mail. • Een belangrijk doel van deze communicatie is voorlichting, waarbij informatie, inzichten, kennis en kunde gedeeld worden en leiden tot handelingsperspectief over allerhande cyberonderwerpen. Een onderdeel hiervan is ook het waarschuwen voor dreigingen en het inzichtelijk maken van risico's. Er is ook behoefte aan een overzicht van de aangeboden hulp en een wegwijzer naar de partijen die deze hulp aanbieden; denk bijvoorbeeld aan slachtofferhulp, de Politie, Toezichthouders, etc.
2	15	**Handelingsperspectief dat aansluit op risicoprofiel** Er is behoefte aan concreet handelingsperspectief dat is gebaseerd op het risicoprofiel van het bedrijf. Dit heeft als doel bedrijven binnen het mkb te helpen met de afweging tussen veiligheid en de benodigde investeringen, ofwel, "wanneer is goed, goed genoeg?". Dit hulpmiddel zou idealiter de volgende informatie bevatten: • De absolute basismaatregelen die voor iedereen gelden. Dit is het laaghangend fruit: cyberweerbaarheidsmaatregelen die gratis of erg goedkoop zijn, makkelijk te implementeren en onafhankelijk van het type bedrijf of het risicoprofiel. Denk bijvoorbeeld aan het maken van een back-up van de belangrijkste bedrijfsgegevens. • Inzicht in welke risico's een bedrijf loopt, en in hoeverre deze zijn afgedekt; of in andere woorden: "een periodieke keuring, zoals een APK". De overheid zou dit verplicht kunnen stellen aan alle bedrijven waarbij een bedrijf bijvoorbeeld elk jaar een vragenlijst in moet vullen om aan te geven welke risico's het bedrijf loopt en welke maatregelen geïmplementeerd zijn. Dit zou eventueel ook via bijvoorbeeld de accountant kunnen, die verplicht wordt te vragen naar de cyberweerbaarheid van het bedrijf bij het opstellen van de jaarverslagen. • Additionele maatregelen die geïmplementeerd moeten/kunnen worden op basis van het type bedrijf en/of risicoprofiel. Deze additionele maatregelen kunnen eventueel verdeeld worden in verschillende niveaus. • Per maatregel (basis en additioneel) een inschatting van de benodigde investeringen. • Per maatregel (basis en additioneel) inzicht in wat het oplevert. • Dit hulpmiddel zou ook kunnen doorverwijzen naar informatiebronnen die nuttig zijn voor maatregelen die bedrijven zelf kosteloos kunnen implementeren. Eventueel kan ook aangegeven worden in hoeverre maatregelen wettelijk verplicht zijn, zoals maatregelen rondom de privacy van persoonsgegevens.
3	10	**Selectie van en omgang met ICT-leveranciers** Er is behoefte aan een overzicht van betrouwbare ICT/cyber-leveranciers die de benodigde producten/diensten kunnen leveren. De overheid wordt gezien als betrouwbaar en onafhankelijk, dus het zou helpen als juist de overheid aangeeft welke commerciële partijen kwalitatieve producten/diensten leveren; dit zou eventueel kunnen aan de hand van een keurmerk die bedrijven kunnen behalen als ze voldoen aan een eisen die de overheid heeft opgesteld. Geïnterviewden geven verder aan behoefte te hebben aan hulp in de omgang met hun ICT-dienstverlener. Hierbij gaat het met name om de beginfase waarin onderlinge verwachtingen worden besproken. Hoe stel je eisen aan je leverancier als je geen expert ben op het gebied van cyberveiligheid? Hoe bepaal je welke diensten en producten nodig zijn, zonder dat de kosten teveel oplopen? Er is behoefte aan "gouden standaarden" die gedeeld kunnen worden met de opdrachtgevers voordat een samenwerking aangegaan wordt. Een simpele checklist om te valideren of een leverancier voldoet aan bepaalde eisen zou al helpen; belangrijk hierbij is dat deze checklist afgestemd wordt op het type bedrijf of risicoprofiel. Verder is er behoefte aan hulp als de samenwerking met de ICT-dienstverlener al verder gevorderd is. Dit om continu te monitoren wat het huidige cyberweerbaarheidsniveau, wat de dreigingen zijn en welke maatregelen geïmplementeerd worden.

#	Ja	Behoefte
4	9	**Financiële ondersteuning** Er is behoefte aan financiële ondersteuning in de vorm van bijvoorbeeld subsidies. Dit geldt niet voor alle bedrijven; sommigen geven aan genoeg middelen te hebben maar willen weten wat een investering oplevert. Naast financiële middelen is het ook belangrijk ondersteuning te krijgen voor het aanvragen of inzetten van deze middelen. Een subsidieaanvraag moet bijvoorbeeld simpel en snel in te vullen zijn. Sommige geïnterviewden geven aan dat de financiële ondersteuning vanuit de overheid gericht moet zijn op preventieve maatregelen. Dat er bijvoorbeeld vouchers voor penetratietesten beschikbaar worden gesteld waarbij de overheid dus een deel van de kosten dekt.
5	7	**Duidelijke regels en handhaving** Geïnterviewden geven aan dat de overheid wel een kader schets voor de cyberveiligheid van bedrijven, maar bedrijven vervolgens hierin vrij laat. De overheid kan beter duidelijke regels/verplichtingen stellen, al is het alleen al op eventuele basismaatregelen. Naast ondersteuning in het naleven van de regels, is ook duidelijke handhaving (opleggen van sancties en het opsporen van criminelen) nodig gezien bedrijven binnen het mkb “vaak pas wat gaan doen als ze op de vingers getikt worden”. Dit alles biedt bedrijven het complete plaatje en zorgt dat ze weten waar ze aan toe zijn.
6	5	**Certificering** Er is behoefte aan een manier waarop een bedrijf aan klanten en leveranciers kan laten zien dat hun cyberweerbaarheid op een voor hen optimaal niveau zit. Er zijn certificaten te behalen zoals de ISO27001, maar deze is niet voor iedereen nodig of haalbaar. Er is behoefte aan een “mini-ISO”. En al heeft een bedrijf deze ISO certificering, dan nog weet niet elke klant wat dat precies betekent.
7	4	**Roadmap/wegwijzer** Er is behoefte aan een duidelijke en complete wegwijzer als het gaat om cyberveiligheid. Bijvoorbeeld rondom NIS2 of andere veranderingen die een impact hebben op bedrijven binnen het mkb. Deze roadmap/wegwijzer kan dan ook een overzicht bieden van alle hulp die er vanuit de overheid aangeboden wordt. Er zijn veel tools en hulpmiddelen, het is alleen niet duidelijk wie wat aanbiedt.
8	3	**Centraal punt met hulplijn** Er is behoefte aan één centraal punt waar alles verzameld is (informatie, hulpmiddelen, advies, uitleg, etc.). En indien een bepaalde dienst/hulpmiddel wordt aangeboden door een andere partij, moet er een doorverwijzing zijn naar die partij. Op deze manier kan iemand die op zoek is naar informatie, erop vertrouwen dat dit centrale punt compleet is. Ook is er behoefte aan de mogelijkheid om dit centrale punt te bellen voor advies en ondersteuning.
9	1	**Screening van buitenlandse kandidaten** Een bedrijf geeft aan behoefte te hebben aan hulp vanuit de overheid bij het screenen van buitenlandse kandidaten voor een openstaande vacature.
10	1	**Incidentbehandeling** Een bedrijf geeft aan dat er meer openheid en transparantie nodig is nadat een incident gemeld is en een onderzoek gestart is.
11	1	**ICT/cyber in het onderwijs** Er is meer aandacht nodig voor ICT/cyber in het onderwijs.
12	1	**Hulp bij herstel** Er is behoefte aan “een helpende hand” na een cyberincident, bijvoorbeeld met slachtofferhulp, het doen van aangifte, fraude melden bij de bank, etc.

Tabel 15 Behoeftes, gesorteerd op het aantal keer dat ze genoemd zijn tijdens interviews.

Variabelen en cyberweerbaarheid

Figuur 13 toont 5 variabelen van de 32 geïnterviewde bedrijven binnen het mkb:

1. Bedrijfsgrootte in termen van het aantal medewerkers;
2. Het wel of niet aanwezig zijn van iemand met een ICT-functie;
3. Het gebruik van enkel SaaS versus SaaS en op maat gemaakte software;
4. Het wel of niet uitbesteden van ICT aan een externe leverancier;
5. De industrie waarin het bedrijf werkzaam is.

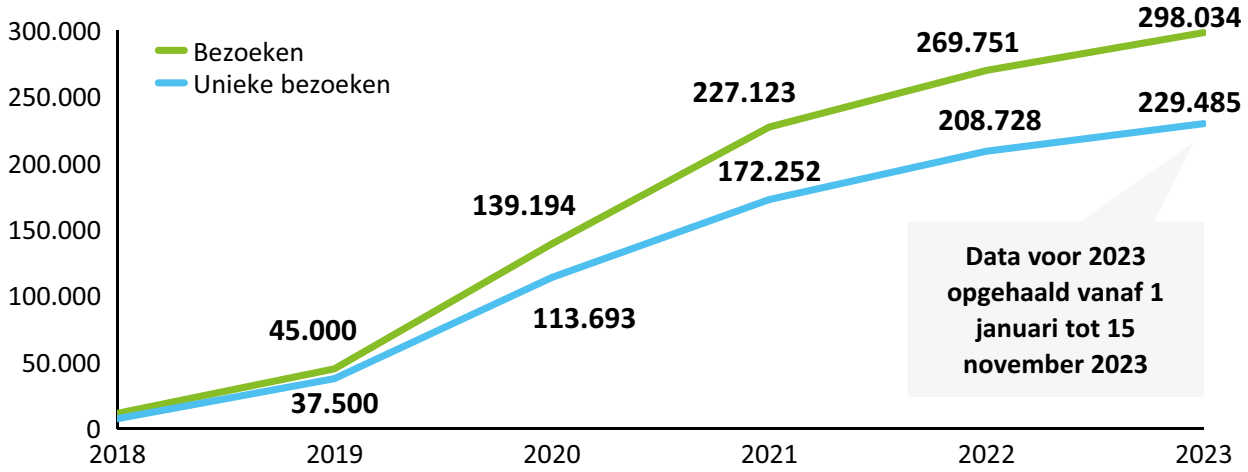
Voor elk van de variabelen wordt ook aangegeven hoeveel bedrijven binnen die categorie een hoge, gemiddelde of lage huidige cyberweerbaarheid hebben. Dit is vastgesteld door middel van de CyberVeilig Check van het DTC.

Figuur 13 Variabelen van geïnterviewde bedrijven en hun cyberweerbaarheid

Appendix G – Gegevens DTC

Figuur 14 toont het totale en unieke aantal bezoeken aan de DTC website vanaf de oprichting in 2018 tot en met 15 november 2023.

Aantal totale en unieke bezoeken aan de DTC website per jaar
Data aangeleverd door het DTC



Figuur 14 Aantal totale en unieke website bezoeken van het DTC, per jaar

Tabel 16 toont de type hulpmiddelen van het DTC en het aantal bezoeken van de desbetreffende internet pagina. De data is opgehaald voor de periode 1 januari tot 15 november 2023, dus de totale aantallen zijn geëxtrapoleerd tot eind december 2023 (zie groene rij onderaan).

	Type hulpmiddel	Hulpmiddel	Bezoeken	Unieke bezoeken	Aantal ingevuld	Aantal reviews
Data voor periode: 1 januari tot 15 november 2023	**Dreigings-informatie**	Nieuws en Cyber Alerts	38.917	-	-	-
		View /cyberalerts	3.005	-	-	-
		RSS feed Nieuws & Alerts	436	-	-	-
	Awareness	Ondernemersverhalen	4.669	-	-	-
		Phishing Bingokaart	929	-	-	-
	Hulpmiddelen	Disaster Recovery Plan	538	-	-	-
		Poster Basisprincipes	416	-	-	-
		Toolkit Cyberincident	386	-	-	-
		Bellijst	598	-	-	-
		Feiten en Fabels	344	-	-	-
	Kennis	Webinars	1.500	-	-	-
	Financiële ondersteuning	Subsidieregeling 'Mijn Cyberweerbare Zaak'	6.753	-	-	-
		Subsidieregeling samenwerkingsverbanden Cyberweerbaarheid	2.333	-	-	-
	Totaal hulpmiddelen excl. Tools		**61.882**	-	-	-
	Tools	Cyberveilig Check voor mkb en zzp	62.699	58.284	6.258	203
		Basisscan Cyberweerbaarheid	7.994	6.821	965	157
		Test je Back-up	495	434	725	-
		Automatisch updaten?	419	389	254	-
		Check je risicoklasse	3.742	3.198	1.945	118
		Is je ICS of OT-security op orde?	813	684	224	12
		Wegwijzer voor cybersecurity initiatieven	1.300	925	434	-
		Phishing Quiz	10.060	8.430	5.231	153
		Phishing Bonus Quiz	2.075	1.929	1.704	-
		Fraude Quiz	2.645	2.240	840	-
		Fraude Bonus Quiz	117	98	66	-
	Totaal Tools		**92.359**	**83.432**	**18.646**	**643**
	Totaal alle hulpmiddelen		**154.241**	-	-	-
Totaal (extrapolatie tot eind 2023)			**177.038**	**95.763**	**21.402**	**738**

Tabel 16 Type hulpmiddelen van het DTC, en het aantal keer dat de desbetreffende internetpagina's bezocht zijn in 2023.

Appendix H – Gegevens NCSC

#	Top 10 zoektermen (1 april 2022 t/m 30 september 2023, 121 dagen)	Aantal
1	TLS	1.079
2	NIS2	886
3	Ransomware	550
4	Kxss1	383
5	Cloud	362
6	Wachtwoord	359
7	Encryptie	348
8	Factsheet	281
9	Phishing	202
10	Richtlijnen	197

#	Top 15 producten (1 juni 2023 t/m 30 september 2023, 547 dagen)	Aantal
1	Ict-beveiligingsrichtlijnen voor webapplicaties	1.903
2	Ict-beveiligingsrichtlijnen voor transport layer security 2.1	1.623
3	Webpagina handreiking cybersecuritymaatregelen (juli tot nov. '23)	1.565
4	Maak je organisatie quantumveilig	1.202
5	Incidentresponsplan ransomware	1.167
6	Risico's in de toeleveringsketen	1.030
7	Handreiking security.txt	654
8	Handreiking cybersecuritymaatregelen	645
9	Infosheet securitytesten	603
10	NLCS 2022	602
11	Volwassen authenticeren	455
12	Factsheet risicobeheersing	407
13	Cybersecuritybeeld Nederland 2023	361
14	Omgaan met ddos-aanvallen van hacktivistische groeperingen	335
15	Factsheet open source security	237
Totaal (zoektermen+producten), omgerekend naar 365 dagen		**26.228**

Tabel 17 Gegevens NCSC

Appendix I – Buitenland

Duitsland

Overheidspartij voor cyber

- Het Bundesamt für Sicherheit in der Informationstechnik (BSI), oftewel het Federale Bureau voor Informatiebeveiliging, is het belangrijkste federale agentschap voor cyberbeveiliging en een vooraanstaande speler in het bevorderen van veilige digitalisering in Duitsland.

Positionering

- Het doel van het BSI is het bevorderen van veilig gebruik van informatie- en communicatietechnologie in de overheid, bedrijven en de samenleving. Ze streven naar ondersteuning van informatiebeveiliging als een essentiële voorwaarde voor digitalisering, met aandacht voor veiligheidsaspecten vanaf de ontwikkeling van IT-systemen.

Wetgeving/richtlijnen

- Network and Information Systems Directive 2 (NIS2): is Europese wetgeving die gericht is op het versterken van cybersecurity in vitale sectoren en digitale dienstverleners. Het beoogt de weerbaarheid tegen cyberdreigingen te vergroten door verplichtingen op het gebied van beveiliging en rapportage op te leggen aan specifieke organisaties binnen de EU.
- BSI-Act: een wet die in 2021 in Duitsland is ingegaan om de beveiliging van kritische infrastructuur te verbeteren. De wet stelt eisen aan bedrijven die essentiële diensten verlenen, zoals energiebedrijven en banken om hun IT-systemen te beschermen tegen cyberaanvallen.

Publiek-private samenwerkingen

- Alliance for Cyber Security: is een samenwerkingsverband tussen bedrijven en overheden dat in 2012 is opgericht. Het doel is om kennis over cybersecurity te delen en samen te werken tegen online dreigingen. Met ongeveer 6.620 deelnemende organisaties is het een belangrijk platform in Duitsland.
- Cyber Security Network: is een vereniging van gekwalificeerde experts in incidentafhandeling. Deze experts zetten hun kennis en expertise in, met als doel het oplossen van IT-incidenten en het verbeteren van de cyberweerbaarheid in Duitsland.
- UP KRITIS: is een samenwerkingsverband tussen exploitanten van kritieke infrastructuur, hun verenigingen en de verantwoordelijke overheidsinstanties.

Meldpunt

- Report- and information portal: is een portal waar je meldingen kan maken van IT-incidenten.

Certificering/keurmerk

- IT-Grundschutz: is een certificering voor de informatiebeveiliging van organisaties. De certificering is gebaseerd op de BSI-IT-Grundschutz-Handbuch, een handboek voor informatiebeveiliging dat door het BSI is ontwikkeld.
- IT-Sicherheitskennzeichen: is een keurmerk voor informatiebeveiligingsproducten en -diensten. Het keurmerk wordt toegekend aan producten en diensten die voldoen aan de eisen van de BSI-IT-Grundschutz-Handbuch.
- BSI-Standard 200-1: Deze standaard beschrijft stap voor stap hoe succesvol informatiebeveiligingsmanagement kan worden opgezet en welke taken het managementniveau in overheidsinstanties en bedrijven in dit verband heeft.
- BSI-Standard 200-2: Deze standaard biedt het BSI methodologie voor effectief informatiebeveiligingsmanagement. Dit kan worden aangepast aan de vereisten van organisaties van verschillende types en groottes.
- BSI-Standard 200-3: Deze standaard biedt het BSI een eenvoudig toe te passen en erkende procedure die organisaties in staat stelt om hun informatiebeveiligingsrisico's adequaat en gericht te beheersen.
- BSI-Standard 100-4: Deze standaard richt zich op Business Continuity Management.
- IT-Sicherheitsgesetz 2.0: is de tweede versie van de wet welke als doel heeft om de beveiliging van IT-systemen te verbeteren.

Subsidie

- Cyber security and digital sovereignty in 5G/6G communication technologies: het MKB kan bij de overheid een subsidie aanvragen voor de implementatie van 5G/6G.Duitsland wilt een marktleider op dit gebied worden en investeert daar (onder andere) op deze manier in.
- Go-digital: deze subsidie ondersteunt bij optimalisatie van processen, gegevensbenutting en biedt financiële steun voor beschermingsmaatregelen tegen gegevensverlies.

Dreigingsinformatie

- Threat report: het jaarlijkse Threat Report van het BSI geeft een overzicht van de dreigingen in cyberspace in Duitsland. In het rapport voor 2023 concludeert de Federale Cyber Security Authority dat de dreiging in cyberspace hoger is dan ooit tevoren.

Database

- FLOSS: is een lijst van gratis en open-source software die wordt gedeeld door het BSI met als doel de beveiliging te verbeteren.

Kennisdeling

- Information papers: het BSI deelt informatieve papers met aanbevelingen over IT-beveiliging, waaronder bijvoorbeeld tips voor bedrijven om zich te beschermen tegen veelvoorkomende dreigingen.
- Technical papers: het BSI deelt technische papers over IT-beveiliging. De technische richtlijnen zijn doorgaans gericht op iedereen die betrokken is bij het opzetten of beveiligen van IT-systemen.

Denemarken

Overheidspartij voor cyber

- Het Center for Cybersikkerhed (CFCS) is een organisatie die bedrijven helpt zich voor te bereiden op cyberdreigingen. CFCS geeft advies over deze dreigingen en over maatregelen die kunnen worden genomen om de veiligheid te vergroten.
- De Danish Business Authority biedt gratis cyberveiligheidsdiensten aan het Deense mkb, waaronder risicobeoordeling, training en ondersteuning bij incidenten.
- Het Digitaliseringsstyrelsen is een Deens overheidsorgaan dat verantwoordelijk is voor de digitale transformatie van de publieke sector.
- Sikkerdigital.dk is een website van de Digitaliseringsstyrelsen die informatie en advies biedt over digitale veiligheid voor burgers, bedrijven en overheidsinstanties Hun initiatieven hebben het doel om bewustwording te creëren over cyberdreigingen en veilig online gedrag te bevorderen. Ook heeft Sikkerdigital een cyber hotline.

Positionering

- Het Nationaal Cyber Security Centrum (CFCS) is de overheidsorganisatie die verantwoordelijk is voor het beschermen van Denemarken tegen cyberbedreigingen.

Wetgeving/richtlijnen

- Network and Information Systems Directive 2 (NIS2): is Europese wetgeving die gericht is op het versterken van cybersecurity. Het beoogt de weerbaarheid tegen cyberdreigingen te vergroten door verplichtingen op het gebied van beveiliging en rapportage op te leggen aan specifieke organisaties binnen de EU.

Publiek-private samenwerking

- Strategisch forum voor samenwerking op het gebied van cyberveiligheid: is een forum op de site van het CFCS waar een groep cyberprofessionals artikelen op schrijft op het gebied van digitale weerbaarheid.
- Cyber Security Pact: is een publiek-privaat partnerschap dat ervoor moet zorgen dat het Deense midden- en kleinbedrijf (MKB) het meest cyberveilige van Europa wordt.

Meldpunt

- Cyberhotline: is er voor burgers en bedrijven die advies willen over hoe ze digitaal veiliger kunnen worden en hoe ze digitale fraude en cyberaanvallen kunnen aanpakken en voorkomen. De cyberhotline is onderdeel van sikkerdigital.dk.

Certificering/keurmerk

- D-seal: fungeert als een universele norm om de beveiligingsstatus van een bedrijf over te brengen. Het is relevant in situaties waar de ISO27001 bijvoorbeeld te omvangrijk is. Deze norm is geschikt voor bedrijven die geen ISO- of NIS-certificering willen behalen, maar toch hun beveiligingsniveau op een herkenbare manier willen communiceren.

Subsidie

- SME: Digital Pool/SMV:DigitalSMV:Digital: Deze subsidiepool ter waarde van in totaal 50 miljoen Deense kronen beoogt de digitale beveiliging te verbeteren door ondersteuning te bieden via adviesdiensten. De pool ging van start op 17 maart 2022 en sloot op 13 september 2022.

Dreigingsinformatie

- Threat Report: CFCS brengt periodiek threat reports uit om iedereen op te hoogte te houden van de actuele dreigingen in het cyberlandschap.

Kennnisdeling

- Bedrijfsgerichte informatiecampagnes: campagnes vanuit de Danish Business Authority die zich richten op bedrijven met betrekking tot cyber- en informatiebeveiliging. Deze initiatieven worden uitgevoerd op diverse platforms, waaronder sociale media, en omvatten evenementen zoals webinars. Dit laatste doet de CFCS ook, zie hier.
- Bedrijvenforum voor digitale veiligheid.
- Cyber Security Council: adviseert de overheid over hoe de digitale veiligheid kan worden versterkt en draagt bij aan kennisdeling tussen overheden, het bedrijfsleven en de onderzoekswereld.
- Sikkerdigital.dk: een website die advies geeft aan burgers en bedrijven op het gebied van cyberveiligheid.

Frankrijk

Overheidspartij voor cyber

- De Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) is het Franse nationale agentschap voor de veiligheid van informatiesystemen. De ANSSI bestaat uit vier departementen: Administratie, Expertise, Operatie en Strategie. Het departement Expertise is verantwoordelijk voor het publiceren van 'best practices' en richtlijnen, het definiëren van technische certificeringsstandaarden en het aanbieden van betrouwbare beveiligingsproducten en -diensten. Het departement Operatie is verantwoordelijk voor het verzamelen, analyseren en delen van dreigingsinformatie. Onder dit departement valt het Franse nationale Computer Emergency Response Team.

Positionering

- Met het oog op 2030 positioneert het ANSSI zich met name als (1) een sleutelspeler in de digitale transformatie en leidend in het vormen van beleid op digitale veiligheid, (2) leidend in de cyberweerbaarheidsketen met versterkte samenwerking met nationale partners, (3) bron van kennis voor onderwijs en training over cyberveiligheid, (4) een partner met het private domein voor het opbouwen van cyber capaciteit.

Publiek-private samenwerkingen

- Cybermalveillance: is een platform waar publieke (ANSSI en verschillende ministeries) en private partijen (bv: branchevereningen, commerciële dienstverleners, cyberslachtoffers, netwerkbeheerders) samenwerken met als doel: (1) cyberslachtoffers ondersteunen door ze door te verwijzen naar professionele cyberveiligheidsorganisaties, (2) bewustwordingscampagnes en ondersteuning voor het beveiligen van informatiesystemen door gecertificeerde dienstverleners (ExpertCyber), en (3) monitoren en analyseren van gebruikersdata.

Meldpunt

- 'Computer Emergency Response Team' (CERT-FR): dat 24/7 fungeert als het contactpunt voor alle cyberincidenten. Het CERT-FR richt zich met name op publieke organisaties en vitale organisaties, niet het brede Franse publiek of het mkb, hiervoor bestaat Cybermalveillance.
- Internet Signalement: hier is het mogelijk om via het Ministry of the Interior een melding te doen van een cyberincident.
- Chatdienst Gendarmerie: hier kun je 24/7, online, in contact komen met de politie om te praten of advies te vragen.

Certificering/keurmerk

- ExpertCyber: is een certificering in samenwerking met auditor AFNOR waar dienstverleners voor 800 euro, 2 jaar lang het label krijgen en in een database komen die publiekelijk toegankelijk is.

Dreigingsinformatie

- Cyber-malware observatory: hier wordt data van cyberincidenten gemonitord

Kennisdeling

- Bewustwordingscampagnes: aangeboden vanuit Cybermalveillance door middel van via nationale tv spotjes.
- Awareness kit: dat negen thema's afdekt in zes verschillende formats (informatiebladen, memo's, posters, stripfiguren, video's, quiz, infographics)
- Request Support: is een online tool waar je op basis van een aantal vragen over een cyberincident doorverwezen wordt naar een professional.
- Artikelen: Cybermalveillance publiceert periodiek artikelen op haar site over allerlei cyberonderwerpen in de vorm van nieuwsberichten, facts and figures.
- Diagnose an incident: is een online tool waar je aan de hand van een aantal vragen kunt bepalen of er een cyberincident heeft plaatsgevonden en wat je moet doen.

Verenigd Koninkrijk

Overheidspartij voor cyber

- Het National Cyber Security Centre (NCSC) is een overheidsinstantie die verantwoordelijk is voor het verbeteren van de cyberbeveiliging van het Verenigd Koninkrijk en biedt begeleiding, ondersteuning en advies aan onder andere het bedrijfsleven.

Positionering

- Het NCSC positioneert zichzelf als de officiële certificeringsinstantie op nationaal niveau. Het doel van het NCSC is om het VK veiliger te maken op het gebied van online activiteiten, wat past binnen de bredere strategie van de overheid om een toonaangevend centrum van wetenschap en technologie te worden.

Wetgeving/richtlijnen

- Cyber Assessment Framework (CAF): is een hulpmiddel voor het beoordelen van de cyberweerbaarheid. Het geeft richtlijnen aan organisaties die verantwoordelijk zijn voor essentiële diensten en activiteiten.
- GovAssure: is de nieuwe aanpak voor het waarborgen van cyberbeveiliging binnen de overheid. Het zal het cyberbeveiligingsaspect van de Departmental Security Health Check vervangen en voldoet aan de eisen van de Cyber Security Strategy van de overheid. GovAssure maakt gebruik van het Cyber Assessment Framework (CAF).

Publiek-private samenwerking

- Industry 100 (i100): is het belangrijkste initiatief van het NCSC om nauwe samenwerking mogelijk te maken met de meest getalenteerde en diverse denkers in de Engelse industrie.
- UK Cyber Cluster Collaboration (UKC3): fungeert als een centraal knooppunt voor publieke en private organisaties, en het bevordert innovatie en groei op het gebied van cyberbeveiliging.

Meldpunt

- Cyber Emergency Incident: is bedoeld voor noodgevallen met betrekking tot cyberdreigingen en incidenten en mag alleen worden gebeld onder bepaalde voorwaarden.
- Cyber Incident Service: is bedoeld om cyberdreigingen en incidenten te melden die geen nood hebben.

Certificering/Keurmerk

- Certified Cyber Professional: een certificering die werd uitgereikt vanuit het NCSC. Deze certificering is een bewijs van de kennis, vaardigheden en ervaring die nodig zijn om een succesvolle carrière in de cyberbeveiliging op te bouwen.
  Echter wordt deze certificering niet meer uitgereikt. Het NCSC is overgestapt naar het UK Cybersecurity Council.
- UK Cybersecurity Council: streeft naar een standaard voor het beroep. De introductie van een universeel erkende professionele standaard voor de industrie is bedoeld om duidelijkheid te verschaffen voor zowel cyberbeoefenaars als werkgevers in het VK die op zoek zijn naar cyberexpertise.
- Cyber Essentials: is een door de overheid gesteund programma dat organisaties, ongeacht hun omvang, helpt beschermen tegen een breed scala aan veelvoorkomende cyberaanvallen.
- IASME: is een partner van het NCSC die organisaties helpt bij het verkrijgen van certificeringen.

Subsidies

- Funded Cyber Essentials Programme: is een financieringsinitiatief voor bedrijven met 1 tot 49 werknemers in specifieke sectoren. Op dit moment is het programma gesloten vanwege een grote vraag.

Dreigingsinformatie

- Connect Inform Share Protect (CISP): is een platform voor cyberbeveiligingsprofessionals in het Verenigd Koninkrijk om samen te werken aan cyberdreigingsinformatie in een veilige omgeving.
- Threat Intel Report

Database

- Verify a supplier: is een lijst van 222 (op het moment van schrijven) geverifieerde producten/diensten. Hierin kun je details vinden over het bedrijf dat de service levert en wat ze precies aanbieden.

Kennisdeling

- Small Business Guide: Cyber Security: is een stappenplan met 5 eenvoudige stappen, elk voorzien van praktische tips om de cyberweerbaarheid te verhogen. Het richt zich op het voorkomen van bedreigingen zoals phishing, malware, etc.
- CyberAware: is een website die informatie en praktische stappen biedt om je beter te beveiligen tegen cyberdreigingen.
- CyberUK: is een event van de Britse overheid op het gebied van cyberbeveiliging, waar elk jaar duizenden leiders en professionals uit de sector samenkomen.

Huidige cyberweerbaarheid

- Free Action Cyber Plan: is VK's versie van de Cyberveilig Check. Door enkele vragen te beantwoorden, zoals over het gebruik van 2FA, back-ups, etc., ontvang je vervolgens een takenlijstje met aanbevelingen waar je aan zou moeten werken om de cyberveiligheid te verbeteren.

Deloitte.