‘Verkleinen van de cyberweerbaarheidskloof’

Advies over de cyberweerbaarheid van het Nederlandse midden- en kleinbedrijf

CSR
Cyber Security Council
Cyber Security Raad

‘Verkleinen van de cyberweerbaarheidskloof’

Advies over de cyberweerbaarheid van het Nederlandse midden- en kleinbedrijf

Gericht aan:

De minister van Justitie en Veiligheid
De minister van Economische Zaken en Klimaat

Kopie aan:

De staatssecretaris Koninkrijksrelaties en Digitalisering

CSR
Cyber Security Council
Cyber Security Raad

mei 2024

INLEIDING

Dit advies is opgesteld in reactie op het verzoek van de minister van Justitie en Veiligheid d.d. 31 januari 2023, waarin zij de Cyber Security Raad (hierna de raad) vroeg advies uit te brengen over de cyberweerbaarheidskloof tussen organisaties. Deze kloof betreft de grote verschillen in cyberweerbaarheid tussen voorlopers (organisaties die hun cyberweerbaarheidsmaatregelen in balans hebben met de dreiging) en achterblijvers (organisaties waarvoor dat niet het geval is). De raad gaat in dit advies in op een breed palet aan vraagstukken, waaronder de vragen van de minister. Doel van het advies is om het kabinet met concrete aanbevelingen in staat te stellen om samen met brancheorganisaties, ICT- en telecomleveranciers en het mkb de cyberweerbaarheidskloof te (helpen) verkleinen en waar mogelijk te overbruggen.

Kern van het advies
De focus van dit advies ligt specifiek op het midden- en kleinbedrijf (mkb), omdat in dat domein relatief veel achterblijvers lijken te zijn. De kern van het advies betreft drie hoofdlijnen, die in het vervolg nader worden uitgewerkt:

1. Realiseer een gerichte, structurele en uniforme aanpak om de cyberweerbaarheid van het mkb te verbeteren. Vanuit publiek-privaat partnerschap en onder regie van de Rijksoverheid kan hiermee meer samenhang tussen verschillende initiatieven ontstaan. Ook kan zo de samenwerking binnen de verschillende netwerken en tussen netwerken onderling worden vergroot.
2. Zorg voor passende hulpmiddelen voor het mkb via bekende en toegankelijke kanalen, om elke organisatie in staat te stellen een optimaal cyberweerbaarheidsniveau te bereiken. Die hulpmiddelen variëren van basismaatregelen en metrieken voor het in kaart brengen van weerbaarheidsniveaus, tot hulp bij de uitvoering van risicoanalyses.
3. Stimuleer bedrijven om hun cyberweerbaarheid te verhogen en maatregelen te (laten) nemen ter verbetering. Maak daarbij gebruik van de genoemde aanpak, aangeboden hulpmiddelen en bestaande producten van ICT- en telecomleveranciers. Aankomende EU-wetgeving heeft daarbij weliswaar een aanjagende werking, maar heeft slechts op een gedeelte van het mkb betrekking.

Het uitgangspunt hierbij is om het gehele mkb te bereiken (dus niet enkel op zoek te gaan naar achterblijvers die in potentie het grootste risico lopen) en de aanpak te baseren op de daadwerkelijke behoeften en belevingswereld van ondernemers binnen het mkb.

Positionering en verantwoording
Dit advies is mede tot stand gekomen op basis van een onderzoek[1] dat door Deloitte in opdracht van de raad is uitgevoerd. Dit onderzoek is grotendeels gebaseerd op literatuuronderzoek en consultatie van mkb'ers, vertegenwoordigers van het mkb, publieke partijen, brancheorganisaties en private netwerkpartners van het mkb. Daarmee kon diepgaand inzicht worden verkregen in de worsteling van het mkb met cybersecurity.

[1] Zie het rapport 'Cyberweerbaarheidskloof - Aanbevelingen voor een cyberweerbaar mkb en het verkleinen van de cyberweerbaarheidskloof in Nederland'. Deloitte mei 2024

Parallel aan het onderzoek van Deloitte heeft ook TNO (in opdracht van het ministerie van Economische Zaken en Klimaat (EZK)) het onderzoek 'Veilig Digitaal Ondernemen'[2] uitgevoerd naar de beweegredenen voor ondernemers om al dan niet in te zetten op verbetering van hun cyberweerbaarheid. Het TNO-onderzoek is grotendeels complementair en elementen hieruit zijn ook relevant voor dit advies van de raad.

Waarom specifiek het mkb

Het mkb is de ruggengraat van onze economie en onmisbaar voor alle grote maatschappelijke transities. 70% van de Nederlanders werkt bovendien in het mkb. Een optimaal cyberweerbaar mkb is daarom van belang voor de ondernemers zelf vanwege de bedrijfscontinuïteit (zonder bedrijf geen verdiensten) en eventuele reputatieschade, maar ook voor de samenleving vanwege de systeemcontinuïteit (afzetmarkt en verdienvermogen van Nederland).

Het mkb is divers; het varieert van bedrijven in de maakindustrie tot leveranciers van onderdelen en halffabricaten en van dienstenleveranciers tot retailers. Ook leveren veel Nederlandse bedrijven binnen het mkb aan buitenlandse klanten of partners, of ze zijn zelf multinational. Het betreft middelgrote, kleine en microbedrijven, tot aan de eenmanszaak. Cybersecurity is hier niet altijd *top of mind* en activiteiten zijn veelal gericht op de *core business* van het bedrijf. Bedrijven missen vaak het inzicht in cybersecurityrisico´s en nemen niet altijd voldoende weerbaarheidsmaatregelen. Ook kan een ondernemer de gevolgen van cyberaanvallen of -incidenten zien als acceptabel ondernemersrisico en om deze reden geen preventieve actie nemen.

Vanwege het voorgaande ziet de raad vier redenen om de focus van dit advies specifiek op het mkb te leggen:

1. Veel van de producten en diensten van het mkb worden breed in de samenleving gebruikt en de maatschappij is afhankelijk van een ononderbroken dienstverlening door bedrijven in het mkb.
2. Het hoge kwaliteitsniveau van de vele verschillende producten en diensten maakt het mkb helaas een bewezen lonend doel voor aanvallen door (cyber)criminelen en statelijke actoren.
3. Bedrijven raken steeds verder onderling verbonden in (waarde)ketens. De zwakste schakel in een keten kan ongewenste toegang bieden tot andere bedrijven. Die zwakke schakels kunnen ook bij het mkb voorkomen.
4. De grote(re) bedrijven hebben veelal zelf kennis over cybersecurity in huis en maken financiële middelen vrij. Bij het mkb is dit veel minder het geval.

Bedrijven binnen het mkb zijn integraal onderdeel van het digitale ecosysteem; los van de maatregelen die ondernemers zelf moeten nemen voor het verhogen van hun cyberweerbaarheid, zijn met name kleine bedrijven sterk afhankelijk van hun ICT- en telecomleveranciers. Met de aanstaande Cyber Resilience Act (CRA) wordt het principe van levering van veilige producten en diensten verankerd in Europese regelgeving. Implementatie van deze wet in Nederland zal ondernemers op dit punt meer ontzorgen en het cyberweerbaarheidsniveau van hun bedrijven gaandeweg verhogen.

Leeswijzer

De drie genoemde hoofdlijnen van het advies worden hierna verder uitgewerkt. Daartoe beschrijft de raad eerst de meest relevante cybersecurityontwikkelingen, inclusief het speelveld met de meest relevante actoren vanuit het perspectief van het mkb. Via een beschrijving van de huidige en gewenste situatie volgt een aantal algemene aanbevelingen om de cyberweerbaarheid van bedrijven blijvend te verhogen en daarmee de cyberweerbaarheidskloof te helpen verkleinen en waar mogelijk te overbruggen. Tenslotte volgt een aantal gerichte adviezen aan de betrokken bewindspersonen.

[2] Hof, T., Van der Kleij, R., & Mergler, S. (2024). Veilig digitaal ondernemen: Inzicht in motivaties en barrières door doelgroepsegmentatie. TNO rapport 2024 R10701.

Ontwikkelingen

Dreiging en risico
Het jaarlijkse Cybersecuritybeeld Nederland (CSBN) laat zien dat de cyberdreiging actueel is, toeneemt in omvang en veroorzaakte schade en niet meer weggaat. De opkomst van artificiële intelligentie (AI) levert, naast mogelijkheden voor geavanceerdere beveiliging, ook nieuwe risico's op: cyberaanvallen nemen toe in schaalgrootte, met meer kans op een infectie. Detectie, respons en herstel worden daardoor ook steeds lastiger en vergen specialistische kennis en vaardigheden die zich concentreren bij grotere organisaties waaronder ICT- en telecomleveranciers.

Het mkb is een gericht doelwit voor digitale aanvallers. De cyberdreigingen komen vooral voort uit aanvallen van criminelen en (in sommige sectoren) van statelijke actoren. Door geopolitieke spanningen zijn dergelijke cyberaanvallen het nieuwe normaal geworden. Statelijke actoren zetten deze middelen in tegen een zeer breed scala aan doelwitten, hetgeen het mkb ook sterk raakt. Onderzoek heeft daarnaast aangetoond dat het veelal afpersing betreft via *ransomware*[3], of het stelen of kopiëren van intellectueel eigendom. Dit heeft zowel betrekking op de kantoorautomatisering (ICT) als operationele technologie (OT), ook wel Industrial Automation and Control Systems (IACS) genoemd.

Die laatste systemen sturen een fysieke component aan en komen veel voor in de procesindustrie. Ook in de maakindustrie is deze technologie veelvuldig aanwezig, zeker met de opkomst van digitalisering in deze sector (´smart industry´). Dit brengt complexe uitdagingen met zich mee voor cybersecurity. Het continueren en veilig houden van dergelijke bedrijfsprocessen vereist specifieke kennis en verschillende vormen van samenwerking[4].

Het bedrijfsrisico dat een suboptimaal[5] cyberweerbaar bedrijf door deze aanvallen loopt, is het (deels) stilvallen van de productie of dienstverlening en mogelijke reputatieschade. Dit heeft impact op het bedrijf zelf, maar ook op klanten, toeleveranciers en andere ketenpartners. De gevolgen van suboptimale cyberweerbaarheid in het geval van zich materialiserende risico's worden dan breder maatschappelijk gevoeld. Het risico bestaat dat een bedrijf door de gevolgen van een aanval op wat langere termijn niet meer levensvatbaar is.

Europese en nationale wetgeving & kaders
Verschillende soorten wetgeving en richtlijnen, veelal binnen de EU vastgesteld en nationaal te implementeren, moeten ervoor zorgen dat we als samenleving voldoende weerbaar zijn tegen cyberdreigingen. In de context van dit advies is vooral de Europese Network and Information Security directive[6] (NIS2-richtlijn) van belang, die zich richt op de verbetering van cybersecurity voor een groot aantal organisaties binnen de EU. Deze richtlijn is eind 2022 gepubliceerd en van kracht voor alle lidstaten per 17 oktober 2024. In Nederland moet deze nog worden geïmplementeerd via een nieuwe versie van de Wet beveiliging netwerk- en informatiesystemen (Wbni). Ook de eerdergenoemde EU-wetgeving voor digitaal veilige producten en diensten (CRA) is in deze context zeer relevant.

De NIS2-richtlijn moet bijdragen aan meer uniformiteit en een hoger niveau van cyberweerbaarheid bij alle bedrijven en organisaties die als essentieel of belangrijk zijn aangemerkt. Het betreft zowel een zorgplicht voor een veilige netwerkinfrastructuur en dienstverlening, als een meldplicht voor

[3] Zie cybersecurity monitor van CBS, 2022/2023: https://www.cbs.nl/nl-nl/publicatie/2023/31/cybersecuritymonitor-2022
[4] Zie ook het eerdere advies van de raad over OT/IACS: CSR Advies 'Industrial Automation & Control Systems (IACS)' - CSR-advies 2020, nr. 2 | Advies | Cyber Security Raad
[5] "Suboptimaal" betekent hier dat het cyberweerbaarheidsniveau van een bedrijf niet in overeenstemming is met de risico´s die het bedrijf bereid is te lopen, of dat deze risico´s niet duidelijk of niet bepaald zijn.
[6] Zie NIS2-directive: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555&qid=1707471344352#d1e1300-80-1

organisaties in het geval van cyberincidenten. Bij de implementatie komt ook de aanwijzing van *incident response*-organisaties en toezichthouders aan de orde, met hun verschillende taken, bevoegdheden en verantwoordelijkheden.

Voor het mkb geldt dat slechts een beperkt aantal bedrijven *direct* onder de NIS2 valt, maar er zijn ook bedrijven die *indirect* met de NIS2 te maken krijgen. Bedrijven die direct onder de NIS2 vallen dienen namelijk cybersecurityeisen aan hun leveranciersketen te stellen, hetgeen veelal bedrijven in het mkb betreft. De NIS2-richtlijn zal vanwege het verplichtende karakter een krachtige aanjager zijn voor bedrijven die als essentieel of belangrijk worden aangemerkt. Dit zal ook gelden voor bedrijven die deel uitmaken van de genoemde leveranciersketen van deze organisaties. Daarnaast is er binnen het mkb nog een derde groep die *geen* extra eisen vanuit de NIS2 opgelegd zal krijgen. Binnen het mkb is er behoefte aan voorlichting en aanvullende informatie over de exacte scheiding tussen organisaties die direct, indirect of niet onder de richtlijn vallen.

De invoering van de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb) is in een vergevorderd stadium[7]. Deze wet geeft het Digital Trust Center (DTC) de bevoegdheden om organisaties die *niet* onder de huidige Wbni vallen te informeren en te adviseren over specifieke kwetsbaarheden, dreigingen en incidenten, die betrekking kunnen hebben op hun netwerk- en informatiesystemen. Over het algemeen betreft dit vooral bedrijven binnen het mkb.

Speelveld

Bedrijven binnen het mkb krijgen te maken met een veelheid aan actoren, organisaties en instanties die kaders kunnen stellen ten aanzien van hun cyberweerbaarheid. Het kan dan gaan om wettelijke vereisten, eisen van ketenpartners, ICT-dienstverleners of (publieke en/of private) aanbieders van hulpmiddelen. Hieronder worden de meest relevante initiatieven in het cybersecurity speelveld voor het mkb besproken.

Overheid

De overheid heeft voor het mkb een stimulerende en aanjagende functie. Doorgaans betekent dit het creëren van randvoorwaarden om het handelen van andere spelers mogelijk te maken. Daarbij past het aangaan van publiek-private samenwerkingsverbanden en het bieden van ondersteuning aan al ontwikkelde initiatieven. De rol van de overheid betreft vooral het uitzetten van een strategische koers, het stellen van kaders en het vertalen van EU-wetgeving voor nationale implementatie.

In het streven naar het verhogen van de digitale weerbaarheid van Nederland, het versterken van het cybersecuritystelsel en het aanpakken van digitale dreigingen heeft het kabinet in 2022 de Nederlandse Cybersecuritystrategie (NLCS) gelanceerd, inclusief een bijbehorend actieplan. Dit geeft voor het mkb het volgende aan[8]:

1. *NCSC en DTC ontwikkelen nieuwe producten en diensten met onder andere aandacht voor inbedding van cybersecurity in het risicomanagementproces; crisispreparatie; incidentrespons en thematische advisering. Deze gedifferentieerde en data gedreven informatie- en kennisproducten en -diensten worden gezamenlijk en laagdrempelig beschikbaar gesteld voor organisaties, op een manier die past bij het volwassenheidsniveau.*
2. *Realisatie van een eerste versie van centrale registers voor cybersecurity-gerelateerde informatie (i.e. type ransomware, kwetsbaarheden).*
3. *Het gebruik van tools, zoals risicoscans, producten en beveiligingsadviezen, inclusief handelingsperspectief, stimuleren onder het mkb onder andere via brancheorganisaties, zoals bij het publiek-private platform Samen Digitaal Veilig.*

[7] Op het moment van publicatie van dit advies moet de Eerste kamer nog instemmen met het wetsvoorstel; de Tweede Kamer is per 19 maart 2024 akkoord.
[8] Actieplan NLCS, p.14: https://www.rijksoverheid.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022---2023

4. *Er wordt één set aan basismaatregelen vanuit de overheid geformuleerd en gepromoot voor vrijwillig gebruik door organisaties.*

Al eerder heeft de raad aangegeven dat de overheid een stevige regierol op zich dient te nemen ten aanzien van de uitvoering van de NLCS, inclusief het verschaffen van helderheid over de wederzijdse verwachtingen in de publiek-private samenwerking[9].

Initiatieven vanuit samenwerkingsverbanden
In samenwerking tussen private partijen en in publiek-privaat verband worden (via een stimulerende rol van het DTC) al veel initiatieven ontplooid om de cyberweerbaarheid van bedrijven (in algemene zin) te verbeteren. Hier is het 'groot helpt klein-principe' van toepassing. MKB-Nederland en VNO-NCW hebben de samenwerking gezocht in het project Samen Digitaal Veilig[10], samen met de ministeries van Justitie en Veiligheid en Economische Zaken en Klimaat. De Kamer van Koophandel (KvK) heeft een LinkedIn portaal voor advies en doorverwijzing naar overheidsinstanties. Verder ontwikkelde Brainport Eindhoven CyRa[11] (Cyber Rating), in samenwerking met het bedrijfsleven (waaronder bedrijven die ook zijn aangesloten bij de in 2022 opgerichte CISO Circle of Trust), FERM Rotterdam, de MKB Cybercampus en TÜV Nord Nederland.

Bovenstaande samenwerkingsverbanden spelen een belangrijke rol in de voorlichting en advisering richting het mkb. De dichtheid hiervan in Nederland is groot, hetgeen mogelijkheden biedt voor het verder uitbouwen van een zogenaamd 'netwerk van netwerken'. Dit sluit aan bij de beoogde doorontwikkeling van het huidige Landelijk Dekkend Stelsel (LDS) tot een overkoepelend 'cyberweerbaarheidsnetwerk'. Hierin komen initiatieven samen op het gebied van preventie, informatie- en kennisuitwisseling, crisispreparatie, incidentafhandeling, alsook leren en oefenen. Brancheverenigingen en andere samenwerkingsverbanden kunnen daarin een belangrijke schakelfunctie vervullen richting het mkb.

Initiatieven vanuit private dienstverlening
Afhankelijk van de beschikbare middelen en de aard van het bedrijf, besteden veel bedrijven in het mkb de zorg voor hun cybersecurity uit aan derde partijen. Dit kan gaan om de diensten van ICT- en telecomleveranciers, waar cybersecurity dan een onderdeel van is. Die diensten bieden voor bedrijven passende mogelijkheden om de basishygiëne op orde te brengen. Dit betekent dat ondernemers kunnen kiezen voor beveiliging tegen virussen en malware[12], maar ook aanvullende beveiligingsoplossingen kunnen inkopen.

Wanneer meer specialistische kennis en expertise nodig is, kan het mkb (naast hierboven genoemde oplossingen) een cybersecuritybedrijf inschakelen voor het beheer van de digitale omgeving. Het betreft (onderdelen van) het complete palet van preventie, detectie, respons en herstel, in combinatie met het vooraf uitvoeren van een adequate risicoanalyse. Grotere bedrijven hebben hier in het algemeen meer aandacht voor. Het inkopen van dergelijke diensten kan een premiekorting opleveren bij het afsluiten van een cybersecurityverzekering, aangeboden door verzekeraars en banken, soms in combinatie met een cybersecuritybedrijf.

Voor bedrijven die hun basishygiëne op orde hebben en meer specialistische kennis en expertise nodig hebben, maar zelf onvoldoende financiële ruimte hebben om met een cybersecuritybedrijf in zee te gaan, is er de mogelijkheid om ad hoc of structureel op contractuele basis advies van een expert in te roepen. Het gaat hierbij vaak om een technische analyse en aanvullend advies, opdat het bedrijf zelf de implementatie daarvan ter hand kan nemen.

[9] Zie CSR Adviesbrief over de Nederlandse Cybersecuritystrategie - Minister van Justitie en Veiligheid | Advies | Cyber Security Raad
[10] Zie Samen Digitaal Veilig
[11] Zie Over ons - Cyra - Cyberrating
[12] Leveranciers mogen dit niet standaard aanzetten zonder expliciete toestemming in verband met wet- en regelgeving.

Leren van het buitenland

Hoewel de nationale structuren en strategieën in het internationale speelveld van elkaar verschillen, zijn de dreigingen en kwetsbaarheden over het algemeen grensoverschrijdend. Landen hebben dus met dezelfde problematiek te maken en de geldende EU wet- en regelgeving is identiek. Nederland kan leren van succesvolle of kansrijke initiatieven uit het buitenland, ondanks dat oplossingen in verschillende landen mogelijk anders zijn. Dit geldt bij uitstek voor *like-minded* landen die bijvoorbeeld ook een vergelijkbare digitaliseringsgraad hebben. De raad beveelt aan om specifieke bevindingen[13] uit deze landen, bijvoorbeeld op het gebied van certificeringen of keurmerken, of over subsidietrajecten, mee te wegen bij het nemen van dergelijke maatregelen.

Huidige situatie

Het onderzoek van Deloitte toont aan dat bedrijven binnen het mkb gemiddeld genomen minder maatregelen implementeren en minder vaak risicoanalyses uitvoeren ten opzichte van het geheel aan bedrijven. Ook het recente WODC-rapport *Evaluatiekader en nulmeting Nederlandse Cybersecuritystrategie*[14] geeft ten aanzien van de uitvoering van de NLCS aan dat de betrokkenheid van het mkb extra aandacht behoeft.

Uit het onderzoek van Deloitte komen verschillende interne en externe obstakels naar voren die bedrijven binnen het mkb ervaren en die verhoging van hun cyberweerbaarheidsniveau in de weg staan. Uit interviews blijkt dat drie interne obstakels de meeste problemen geven:

- Er is onvoldoende cyberbewustzijn en -kennis;
- Er is onvoldoende inzicht in de risico's en in mogelijk handelingsperspectief;
- Het is lastig om te bepalen hoeveel en waarin moet worden geïnvesteerd.

In het verlengde van dit onderzoek geeft de raad een aantal aanvullende observaties, die de huidige situatie kenmerken en een optimale cyberweerbaarheid van het mkb in de weg staan:

- De initiatieven die de afgelopen jaren vanuit de overheid, samenwerkingsverbanden en brancheorganisaties zijn ontplooid zijn vaak niet specifiek gericht op het mkb, een bepaalde sector, of een type bedrijf.
- Er is geen of weinig inzicht in de effectiviteit van de aangeboden hulpmiddelen.
- Het geheel aan hulpmiddelen dat wordt aangeboden is onoverzichtelijk, weinig samenhangend en sluit onvoldoende aan bij de behoeften van het mkb. In het aanbod ligt de nadruk op risico-inventarisatie en het creëren van inzicht en is er minder aandacht voor standaard beschikbare oplossingen voor ondernemers.
- De hulpmiddelen die worden aangeboden richten zich voornamelijk op preventieve (inhoudelijke) maatregelen, en niet op het voorbereid zijn op een incident en hoe te handelen tijdens een incident om de impact zo klein mogelijk te houden/maken.
- Sommige ondernemers nemen bewust het risico om niet verder te investeren in hun cyberweerbaarheid.
- Uit angst voor imagoschade zien bedrijven soms af van het melden van een cyberaanval of -incident, of van het doen van aangifte. Dit heeft tot gevolg dat potentiële andere mogelijke slachtoffers niet worden gewaarschuwd of tijdig kunnen worden beschermd[15].
- Niet alle meldingen en/of aangiften kunnen door de politie en het Openbaar Ministerie worden opgepakt, vanwege schaarse capaciteit. Meldingen en aangiften zijn echter cruciaal, omdat ze bijdragen aan een scherper beeld van de actuele trends en ontwikkelingen op het gebied van cybercriminaliteit. Hierdoor is een meer effectieve en efficiënte inzet van capaciteit mogelijk.

[13] Het onderzoeksrapport van Deloitte biedt hier ook aanknopingspunten voor, zie Appendix I.
[14] Zie Evaluatiekader en Nulmeting Nederlandse Cybersecuritystrategie (NLCS) | Rapport | Rijksoverheid.nl
[15] Uit het onderzoek blijkt dat binnen het mkb in het Verenigd Koninkrijk het uitbesteden van ICT leidt tot een vermindering in het melden van incidenten. Of dit ook geldt in de Nederlandse context is onbekend en zou nader onderzocht kunnen worden.

Het onderzoek toont verder aan dat ondernemers binnen het mkb het bereiken van een voor hun optimaal cyberweerbaarheidsniveau in de eerste plaats zien als hun *eigen* verantwoordelijkheid, passend bij het eigen ondernemersrisico. De raad onderschrijft dit, maar om dit goed in te kunnen richten ligt er ook een verantwoordelijkheid bij hun ICT- en telecomleveranciers en andere vertrouwde partners, én moeten onderliggende producten waar zij gebruik van maken aantoonbaar voldoende digitaal veilig zijn.

Sommige bedrijven zien daarnaast een duidelijke coördinerende, faciliterende en verbindende rol voor de overheid weggelegd, bijvoorbeeld als het gaat om bewustwording, het bieden van concreet handelingsperspectief dat aansluit bij de precieze context van het mkb en hulp bij het bepalen waarin geïnvesteerd moet worden. Daarbij hoort ook ondersteuning bij het vaststellen van de eisen waaraan hun ICT- en telecomleveranciers en/of cybersecuritybedrijven moeten voldoen, en het wijzen op standaard beschikbare beveiligingsoplossingen.

Optimale situatie

In een optimale situatie beschikt Nederland over een mkb waarbinnen bedrijven zich bewust zijn van cybersecurityrisico´s en de potentiële impact daarvan op hun bedrijfsprocessen. Daarbij kunnen die bedrijven eigen risicoafwegingen maken voor het (laten) nemen van cybersecuritymaatregelen en zijn ze in staat om zelf te bepalen welke investeringen daarbij horen. In deze situatie krijgen bedrijven op een laagdrempelige manier de benodigde informatie, voorlichting en adviezen. Dit impliceert dat de geïdentificeerde obstakels – zoals hierboven beschreven - zijn weggenomen.

In het geval een bedrijf slachtoffer wordt van cybercriminaliteit is er een *incentive* aanwezig om een aanval te melden en/of aangifte te doen. Daarnaast wordt informatie over kwetsbaarheden gedeeld met andere bedrijven om (potentiële) slachtoffers te waarschuwen. Hierin is een belangrijke rol weggelegd voor de organisatie die voortkomt uit de samenvoeging van het DTC, NCSC en CSIRT-DSP, als centraal expertisecentrum en informatieknooppunt. Door deze fusie worden alle organisaties in Nederland – groot of klein, publiek of privaat, vitaal of niet-vitaal – vanuit één instelling van passende informatie en kennis voorzien. Meer specifiek ziet een optimale situatie er volgens de raad als volgt uit:

- Overheid, brancheorganisaties of samenwerkingsverbanden bieden bedrijven passende hulp om obstakels in de verbetering van hun cybersecurity weg te nemen.
- De hulpmiddelen zijn gemakkelijk toegankelijk; verspreiding vindt idealiter vanuit één loket plaats, via kenniscentra en schakelorganisaties in het eerdergenoemde ´netwerk van netwerken´.
- Het mkb is daardoor in staat risico's te analyseren en bedrijven die open staan voor verbeteringen voor cybersecurity kunnen passende maatregelen treffen. Als onderdeel daarvan kunnen ze digitale producten en diensten afnemen waarvan het beveiligingsniveau past bij die risicoanalyse.
- Naast ICT- en telecomleveranciers fungeren andere partijen in de directe omgeving van bedrijven in het mkb als aanjager door extra aandacht te vragen voor cybersecuritymaatregelen. Dit geldt bijvoorbeeld voor vertrouwde partners zoals verzekeraars, banken, de KvK, accountants en auditors.
- Er is sprake van een monitoringssystematiek voor digitale weerbaarheid, waarin nadrukkelijk ook een plaats is voor het mkb. Hiermee kan gevolgd worden hoe de cyberweerbaarheid van het mkb zich ontwikkelt en of de aangeboden hulpmiddelen het gewenste effect sorteren.

ADVIES

De welvaart van Nederland is gebaat bij een florerend mkb. Optimale cyberweerbaarheid is daarvoor een randvoorwaarde. Binnen het mkb zien we echter aanzienlijke verschillen, in termen van koplopers en achterblijvers in cyberweerbaarheid. Sommige bedrijven accepteren bewust grote cybersecurityrisico´s als onderdeel van hun gehele bedrijfsvoering en zullen op korte termijn niet verbeteren, terwijl andere bedrijven welwillend zijn, maar tekortschieten qua bewustzijn en kennis. Het bereiken van de optimale situatie is dan ook geen geplaveid pad en vereist gezamenlijke inspanningen. Langs de eerdergenoemde drie hoofdlijnen geeft de raad hieronder een aantal algemene adviezen voor verbetering.

1. **De overheid draagt zorg voor een specifiek op het mkb gerichte, structurele en uniforme aanpak via het uitbouwen van het ´netwerk van netwerken´, op grond van bestaande structuren en het duidelijk beleggen van verantwoordelijkheden.**
2. **De overheid, brancheorganisaties en samenwerkingsverbanden bieden passende hulpmiddelen aan via toegankelijke kanalen.**
3. **De overheid stimuleert via publiek-private samenwerking bedrijven binnen het mkb om hun cyberweerbaarheid samen met vertrouwde partners zoveel mogelijk te verhogen, en zet daarbij direct of indirect (bijvoorbeeld via brancheorganisaties) aan tot handelen.**

Ad 1. Draag zorg voor een specifiek op het mkb gerichte, structurele en uniforme aanpak.

In de huidige aanpak om de cyberweerbaarheid van het mkb te verhogen, komen waardevolle initiatieven naar voren, maar samenhang in de organisatie ervan ontbreekt nog grotendeels. De opbouw van een ´netwerk van netwerken´ vanuit bestaande structuren, waarbij de overheid samenwerkt met branchеverenigingen, andere samenwerkingsverbanden en schakelorganisaties, is daarvoor cruciaal.

Gericht
De veelheid aan instanties maken het onoverzichtelijk voor bedrijven in het mkb om informatie, hulpmiddelen of adviezen over cybersecurity goed te vinden en te overzien. Het is daarom noodzakelijk om meer structuur aan te brengen in het netwerk van partijen die een rol spelen in de cyberweerbaarheid van het mkb.

De organisatie die voortkomt uit de samenvoeging van het DTC, NCSC en CSIRT-DSP moet een centrale en coördinerende positie in de uitvoering hiervan innemen, gericht op alle noodzakelijke cybersecurityactiviteiten van organisaties: preventie, detectie, (incident) respons, en bevordering van het herstel- en leervermogen. Enerzijds gaat het daarbij om het (door-)delen van informatie over dreigingen, incidenten en kwetsbaarheden aan het mkb en/of hun partners (ICT- en

telecomleveranciers, cybersecuritybedrijven) en anderzijds om de functie van loket en kenniscentrum voor hulpmiddelen en adviezen over het belang van cybersecurity en de te nemen maatregelen. De beoogde doorontwikkeling van het Landelijk Dekkend Stelsel naar een overkoepelend cyberweerbaarheidsnetwerk geeft daarvoor goede aanknopingspunten, ook in het bereiken van het mkb.

Structureel
De samenwerking binnen dit netwerk dient structureel van aard te zijn, met duidelijke taken en verantwoordelijkheden. Daarbij is het van groot belang om periodiek te evalueren of maatregelen en initiatieven effectief zijn voor het structureel verhogen van de cyberweerbaarheid van het mkb; ook hier zal de welwillendheid en/of het bewustzijn van de betreffende ondernemers een rol spelen.

Vertrouwde partners van bedrijven binnen het mkb die structureel met hen samenwerken, hebben de kans om het nemen van (extra) cybersecuritymaatregelen onder de aandacht te brengen bij hun klanten, en daaraan ook eisen te stellen. Hetzelfde geldt voor een organisatie, zoals de KvK, die met name beginnende ondernemers kan wijzen op hun eigen verantwoordelijkheid en bewust kan maken van cybersecurityrisico´s.

Uniform
Het mkb ervaart over het algemeen hoge regeldruk, terwijl ondernemers in de eerste plaats bezig zijn met het runnen van hun bedrijf. Om het brede palet aan cybersecuritymaatregelen zo overzichtelijk mogelijk te maken is een uniforme aanpak noodzakelijk. Maatwerk kan nodig zijn, bijvoorbeeld wanneer een bedrijf of sector een bijzonder risicoprofiel heeft vanwege hun gevoelige informatie of intellectueel eigendom. Indien specifieke tools op die bedrijven toegespitst moeten worden, kan het nodig zijn om te differentiëren per sector, keten of regio. Brancheorganisaties en specifieke samenwerkingsverbanden spelen een belangrijke rol wanneer differentiatie noodzakelijk is.

Ad 2. Bied passende hulp aan het gehele mkb, via toegankelijke kanalen.

Zoals omschreven in het onderzoek van Deloitte, kan passende hulp worden geboden aan het mkb door een sterke verbinding tussen de onder punt 1 genoemde centrale fusieorganisatie en netwerkpartners die dichtbij bedrijven in het mkb staan. Dit moet leiden tot een compact en uniform geheel aan basismaatregelen. Deze hulpmiddelen dienen gericht te zijn op het uitvoeren van een risicoanalyse die het bedrijf in staat stelt te komen van het huidige naar het optimale cyberweerbaarheidsniveau. Het gaat hierbij om het complete aanbod van hulpmiddelen voor preventie, detectie, (incident)respons, herstel- en leervermogen.

Met de benodigde ondersteuning en voorlichting kunnen bestaande metrieken voor het in kaart brengen van cyberweerbaarheidsniveaus vanuit de private sector, zoals CyRa, maar ook verschillende tools van het DTC, als basis en de facto standaard dienen om te komen tot een praktische invulling die past bij de behoeften van het mkb. Dit sluit nauw aan bij de genoemde vier acties uit de NLCS die direct betrekking hebben op de weerbaarheid van het mkb.

Het is daarbij wel noodzakelijk om het huidige aantal hulpmiddelen terug te brengen en de raad beveelt aan te komen tot een via publiek-privaat partnerschap ontwikkelde handreiking of wegwijzer die brancheorganisaties en hun leden helpt de weg naar de meest passende hulpmiddelen te vinden. Bovendien is een mechanisme nodig dat hulpmiddelen periodiek evalueert op de waarde van hun bijdrage aan de cyberweerbaarheid van de afnemers.

ICT- en telecomleveranciers en cybersecuritybedrijven spelen een belangrijke rol in het verhogen van de cyberweerbaarheid binnen het mkb, bijvoorbeeld door afnemers te informeren over kwetsbaarheden en daarvoor passende oplossingen te implementeren. Afnemers hebben met name behoefte aan hulp bij het selecteren van ICT-leveranciers die voldoende cybersecuritykennis en -kunde hebben en daarmee een waardevolle partner op dit gebied kunnen zijn. Dit kan worden vergemakkelijkt door aansluiting te zoeken bij een kwaliteitskeurmerk voor ICT-leveranciers dat binnen het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) in ontwikkeling is. Ook het gebruik van standaard hulpmiddelen om de juiste vragen en eisen aan leveranciers te kunnen stellen is een goede optie, zoals de door het DTC beschikbaar gestelde checklist voor Service Level Agreements.

Ad 3. Stimuleer en zet aan tot handelen.

Het verbeteren van de aanpak en het aanbod aan hulpmiddelen zijn belangrijke stappen, maar om te komen tot verbetering spelen meerdere factoren een essentiële rol: de motivatie bij ondernemers, ondersteuning via eerdergenoemde vertrouwde partners in hun omgeving én een passend aanbod aan veilige producten en diensten van ICT- en telecomleveranciers.

Het onderzoek van Deloitte heeft niet aangetoond dat bedrijven die actief op zoek gaan naar hulpmiddelen of voorlichting de benodigde informatie onvoldoende kunnen vinden en dat daar dus per definitie de grootste winst te behalen is. Het is bij uitstek de uitdaging om ook die ondernemers te bereiken die van nature geen reden zien om in actie te komen, ongeacht de kwaliteit en vindbaarheid van hulpmiddelen. Deze groep neemt soms weloverwogen het risico op diefstal van gegevens, uitval of zelfs faillissement ten gevolge van een cyberaanval voor lief.

Het is noodzakelijk dat bedrijven op alle niveaus binnen het mkb doordrongen zijn van het belang van cybersecurity, daarvoor daadwerkelijk passende maatregelen nemen en bovendien periodiek een risicoanalyse uitvoeren. Als ondernemers prikkels ervaren vanuit hun ketenpartners en bijvoorbeeld toeleverancier zijn van andere (grotere) bedrijven, is de kans groter dat ze hierop gaan acteren.

Op grond van het bovenstaande, beveelt de raad aan om rekening te houden met de verschillende factoren die het gedrag van ondernemers verklaren en die voor hen bepalend zijn voor het al dan niet tot handelen overgaan. Het TNO-onderzoek 'Veilig Digitaal Ondernemen' geeft hiervoor goede indicaties en stelt ook een aantal interventies voor, afhankelijk van die gedragsfactoren. Drijfveren om te handelen kunnen ook per type organisatie verschillen en hangen bijvoorbeeld samen met kennis, gelegenheid en motivatie.

Bedrijven die niet direct of indirect onder de toekomstige NIS2 vallen zullen vaker achterblijver zijn in termen van de cyberweerbaarheidskloof. De raad beveelt aan om extra aandacht aan deze grote groep bedrijven te geven via stimulerende maatregelen. Brancheorganisaties of samenwerkingsverbanden kunnen hier een belangrijke rol spelen via voorlichting, training en het trekken van lering uit incidenten die zich voordoen bij collega-ondernemers in dezelfde sector. Ook de gerichte inzet van subsidies kan helpen, conform enkele recente trajecten van het DTC. Ondanks dat hiermee slechts een beperkte groep bedrijven bereikt zal worden, bestaat er wel de wens om hiermee te blijven experimenteren.

GERICHTE ADVIEZEN

Onderstaande adviezen zijn bedoeld als concrete invulling van de eerdergenoemde drie hoofdlijnen. Ze zijn gericht op de overheid en via de overheid op de markt. Publiek-private samenwerking is daarbij de hoeksteen voor het versterken van de cyberweerbaarheid van het mkb. Het betreft een gezamenlijke inspanning om de huidige cyberweerbaarheidskloof tussen voorlopers en achterblijvers te verkleinen, waar mogelijk te overbruggen en het mkb over de volle breedte te versterken.

Doelstellingen en acties uit de NLCS die gericht zijn op bescherming van het mkb dienen daarbij extra aandacht te krijgen en voortvarend opgepakt te worden. Dit voorkomt onnodige risico´s, is van groot belang voor de samenleving als geheel en bevordert een stabiele bijdrage van het mkb aan het verdienvermogen van Nederland. Om hier goed invulling aan te kunnen geven, komt de raad tot onderstaande gerichte adviezen.

De raad adviseert in het kader van een **gerichte, uniforme, structurele aanpak** aan de ministers van Justitie en Veiligheid (JenV) en Economische Zaken en Klimaat (EZK) gezamenlijk:

1. Werk vanuit de huidige samenwerking van NCSC, DTC en CSIRT-DSP stapsgewijs toe naar één loket en kenniscentrum in de nieuwe organisatie, dat ook gerichte ondersteuning aan het mkb biedt. Stimuleer daarbij ook doelwit- en slachtoffernotificatie voor het mkb en het doen van meldingen en/of aangiften. Geef extra aandacht aan een adequate inzet van middelen hiervoor.

2. Bundel de krachten van organisaties via uitbouw van het ´netwerk van netwerken' in publiek-private samenwerking (waarbij groot klein helpt) en geef daarin ook vertrouwde partners van het mkb een plek, zoals accountants en de Kamer van Koophandel. Naast de ontwikkeling van informatie- en kennisproducten voor het mkb is het gebruik van standaard beschikbare oplossingen van ICT- en telecomleveranciers cruciaal.

3. Initieer vanaf 2025 een jaarlijkse meting van de cyberweerbaarheid van het mkb en het effect van genomen maatregelen en initiatieven. Maak daarbij gebruik van de recent gepubliceerde nulmeting en koppel dit ook aan de jaarlijkse voortgangsrapportage van de NLCS. Ga daarbij specifiek in op de acties die betrekking hebben op het mkb.

De raad adviseert in het kader van het aanbieden van **passende hulp**:

Aan de ministers van JenV en EZK gezamenlijk:

4. Geef de nieuwe centrale fusieorganisatie het voortouw om in publiek-private samenwerking het aanbod van hulpmiddelen ter verhoging van de cyberweerbaarheid beter af te stemmen op de behoefte van het mkb. Laat dit in overleg met onder andere MKB-Nederland oppakken. Zet voor eind 2024 een harmonisatie daarvan in gang, gericht op een beperking van het huidige aantal verschillende hulpmiddelen.

5. Werk op vrijwillige basis toe naar standaardisatie van hulpmiddelen en maak deze zo laagdrempelig mogelijk. Daarvoor zijn verschillende mogelijkheden, zoals CyRa (Cyber Rating). Stimuleer ook het gebruik van bestaande OT-standaarden en de generieke ISO27001 beveiligingsstandaard (als mogelijke *top-up* op CyRa), en meet de effectiviteit van deze hulpmiddelen. Houd hierbij rekening met (toekomstige) EU-keurmerken en implementeer zo spoedig mogelijk aankomende EU-regelgeving voor veilige producten en diensten.

6. Stimuleer het gebruik van (gedifferentieerde) hulpmiddelen en het nemen van basismaatregelen binnen sectoren. Een toegankelijke handreiking gericht op brancheorganisaties is daarvoor essentieel. Dit geldt ook voor de beveiliging van OT-systemen (ofwel IACS) binnen het mkb; baseer deze zoveel mogelijk op standaard beschikbare oplossingen. Maak hierbij gebruik van bestaande samenwerkingsverbanden.

Aan de minister van EZK:

7. Zie erop toe dat de al in gang gezette ontwikkeling van een kwaliteitskeurmerk voor ICT-leveranciers (in samenwerking met het DTC en brancheorganisaties) wordt geëffectueerd, inclusief cybersecurityeisen, en dat het CCV de uitvoering daarvan voortvarend ter hand neemt. Harmoniseer indien mogelijk een dergelijk keurmerk met toekomstige EU-ontwikkelingen op dit gebied.

De raad adviseert in het kader van **het stimuleren en aanzetten tot handelen**:

Aan de ministers van JenV en EZK gezamenlijk:

8. Overweeg de start van een brede maatschappelijke publiekscampagne in samenwerking met private partijen. De overkoepelende boodschap is daarbij dat ook ondernemers zich moeten aanpassen aan de verder digitaliserende samenleving, met cybersecurity als belangrijk aandachtspunt. Maak daarbij ook gebruik van het TNO-onderzoek 'Veilig Digitaal Ondernemen' om gedrag effectief te kunnen beïnvloeden.

9. Zet in op een tijdige doorvertaling van de NIS2-richtlijn in Nederland en stimuleer specifiek het mkb in het nemen van maatregelen om aan deze eisen te kunnen voldoen. Geef daarbij ook aandacht aan bedrijven die niet vallen onder de huidige Wbni of toekomstige NIS2, waarbij de aanstaande wetgeving (Wbdwb) voor informatiedeling en ondersteuning als uitgangspunt geldt.

's-Gravenhage,

Namens de Cyber Security Raad,

Theo Henrar
(Waarnemend) Covoorzitter CSR

Pieter-Jaap Aalbersberg
Covoorzitter CSR