Kapteynstraat 1, SBIC - Building
suite 220 / 2201 BB Noordwijk

info@cyberveilignederland.nl
www.cyberveilignederland.nl

KvK 71802525

Noordwijk, 11 juni 2024
Ref.: DK/904-0606

Reactie Cyberveilig Nederland op de Cyberbeveiligingswet (Cbw).

De Cyberbeveiligingswet (verder 'Cbw') implementeert de Europese NIS2-richtlijn. De NIS2 beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken.

Cyberveilig Nederland (verder CVNL) is positief over het wetsvoorstel dat voortvloeit uit de richtlijn. Het doel van de richtlijn *"om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren"* zien we terug in het wetsvoorstel en de Memorie van Toelichting (verder MvT). Wij zien echter enkele aandachtspunten, of punten die verduidelijking behoeven, bijvoorbeeld in de vorm van een uitwerking in een algemene maatregel van bestuur (AMvB). Deze verduidelijking vragen wij omdat wanneer de Cbw verschillend wordt geïnterpreteerd, er jurisprudentie nodig zal zijn om bepaalde onduidelijkheden in de Cbw uitgekristalliseerd te krijgen in de praktijk. Dat soort processen zorgen voor jarenlange onduidelijkheid en ongewenste vertraging.

CVNL vraagt in het bijzonder aandacht voor:

1. Het belang van het over en weer uitwisselen met de verschillende CSIRTS's van informatie over dreigingen en kwetsbaarheden met organisaties in het veiligheids- en inlichtingendomein die niet onder de Cbw vallen.

2. Een verdere uitwerking van de taken van de CSIRT's, met name rondom incidenten(afhandeling).
3. Het belang van het waarborgen van de vertrouwensrelatie die een cybersecuritydienstverlener heeft met haar klant/entiteit vallende onder de Cbw.
4. Het verder uitwerken van ketenafhankelijkheid.
5. Het verder uitwerken van de zorgplicht en dan met name rondom de te nemen maatregelen en de waarde van het gebruik van normen/standaarden.
6. Het onzes inziens onterecht ontbreken van detectie/monitoring-maatregelen vanuit entiteiten teneinde de meldplicht in de Cbw op een effectieve manier in te vullen.

Bovenstaande, en overige punten worden hieronder verder uitwerkt, waarbij we voor de leesbaarheid deze hebben onderverdeeld in de onderwerpen *CSIRT*, *meldplicht*, *bestuurder*, *toezicht*, *entiteiten* en *overig*.

CSIRT

- In artikel 6 van de concept Cbw staat beschreven welke overheidsinstanties niet onder de Cbw gaan vallen. Dit betreft overheidsorganisaties 'die in hoofdzaak activiteiten uitvoeren op het gebied van veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. CVNL begrijpt dat de meeste van deze organisaties niet onder de beoogde wet vallen en merkt de volgende zaken op:
  - Veel van deze organisaties hebben zelf diepgaande kennis van dreigingen en kwetsbaarheden, vanwege de aard van hun werkzaamheden. CVNL zou daarom graag (bijvoorbeeld in de MvT) een uitbreiding in de tekst zien waarin deze organisaties actief worden gestimuleerd om deze kennis en informatie actief te delen met de CSIRT's en andere relevante partijen en niet alleen de ontvanger kunnen zijn van deze informatie.
  - In artikel 5.6.6 van de MvT staat dat als de inlichtingen- en veiligheidsdiensten informatie verzoeken bij CSIRT, ze automatisch een relevante partij worden waarmee informatie mag worden gedeeld worden. CVNL is van mening dat wanneer het informatie betreft die de CSIRT van een entiteit heeft ontvangen, deze te allen tijde hiervan in kennis gesteld moet worden.

- In artikel 17 en 18 van de Cbw staan de taken van het NCSC in beschreven, zoals het zijn van coördinator met het oog op het gecoördineerd bekendmaken van kwetsbaarheden. Daarnaast neemt het NCSC-taken op zich die volgen uit de NIS2-richtlijn zoals het fungeren als het centrale contactpunt, het nationale register en het

beheren van een meld- en registratiefunctionaliteit (artikel 22 Cbw). In de MvT staat beschreven dat ‘in de praktijk het NCSC in binnen- en buitenland als “nationale CSIRT” zal opereren’ (5.7.6). CVNL zou graag willen dat het NCSC expliciet wordt aangewezen als nationale CSIRT, al dan niet in de AMvB, aangezien onduidelijkheid over het mandaat (van het NCSC) en welke organisatie nationale CSIRT is in het verleden tot veel onduidelijkheid en discussie heeft geleid en met de huidige formulering deze onduidelijkheid ongewenst blijft voortduren.

- In artikel 17 van de Cbw staan de taken van CSIRT’s omschreven. Eén van de taken is het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële of belangrijke entiteit (17.2.c). Dit vindt CVNL een goede zaak. Echter:
  - Bij een majeure (sector overstijgende) crisis verwacht CVNL dat de (kwalitatieve en kwantitatieve) capaciteiten van de verschillende CSIRT’s onvoldoende zijn en ziet hiervoor de volgende oplossingen:
    - Maak voor deze bijzondere omstandigheden op voorhand een verdringingsreeks, zodat in een daadwerkelijke crisissituatie op basis van deze verdringing een keuze gemaakt kan worden in de bijstandsverzoeken van een CSIRT.
    - De CSIRT’s zoals omschreven in de MvT (artikel 5.6.1) zouden aan een noodzakelijk minimum aan taken en expertise moeten voldoen. Welke taken dit precies zijn zou in een AMvB specifieker uitgewerkt moeten worden.
  - Het is niet duidelijk omschreven wie de coördinatie heeft bij een majeur (sector overstijgend) incident. Crisiscoördinatie is een complex vak dat gedegen kennis en kunde vraagt. Blijft de belangrijke of essentiële entiteit altijd de lead voor het managen van de crisissituatie? Of zal in sommige gevallen een CSIRT deze coördinatie overnemen? Wanneer dit het geval is kan dat tot gevolg hebben dat CSIRT’s controle moeten overnemen bij mitigatie van cross-sectorale incidenten. Dat kan dan weer gevolgen hebben voor de activiteiten of het functioneren van de entiteit die is geraakt door het incident. CVNL zou graag beschreven zien of en hoe een CSIRT de lead mag overnemen bij bepaalde incidenten, wanneer dit inderdaad het geval is en wat daarvan de mogelijke consequenties zijn.
  - In zowel de Cbw als de MvT staat niet duidelijk omschreven wanneer er sprake zal zijn van de opschaling van een incident (bij een entiteit) naar een crisis. Er moet beter omschreven worden welke fasering er bestaat in een opschaling en wat dit betekent voor het al dan niet (meer) autonoom mogen handelen van een entiteit, al dan niet in de AMvB.

- Het CSIRT krijgt verschillende instrumenten om in te zetten:
  "*Indien van toepassing:*
  - *het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële entiteit of belangrijke entiteit;*
  - *het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;*
  - *het op verzoek van een essentiële entiteit of belangrijke entiteit proactief scannen van het netwerk- en informatiesysteem van de betrokken entiteit om kwetsbaarheden met mogelijk significante gevolgen op te sporen;"*

  In zowel de Cbw als de MvT komt niet duidelijk naar voren wanneer het instrumentarium ingezet mag worden en welk servicelevel een entiteit mag verwachten van een CSIRT. Hoe verhoudt dit instrumentarium zich tot het gebruik van commerciële diensten die cybersecuritydienstverleners aanbieden die overeenkomen met dit instrumentarium?

- Artikel 21 Cbw gaat over een nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons. Een cybercrisis of -incident uit zich vaak in de fysieke wereld en omgekeerd. CVNL mist in de Cbw of MvT de relatie met de nationale crisisbeheersing.

- In artikel 39 Cbw staat het volgende beschreven: "*het CSIRT respectievelijk de bevoegde autoriteit kan, na raadpleging van de betrokken entiteit, het publiek informeren over een significant incident of de entiteit verplichten om dit te doen, wanneer:*
  a. publieke bewustmaking nodig is om een significant incident te voorkomen;
  b. dat nodig is om een lopend incident te beheersen; of
  c. de bekendmaking van het significante incident anderszins in het algemeen belang is."

  CVNL vindt dit een goede zaak, aangezien er veel meer openheid moet komen rondom incidenten:
  - Er zijn situaties voorstelbaar waarin terughoudendheid nodig is in het openbaren van incidenten. Worden in de AMvB('s) deze uitzonderingen beschreven?

- Voor CVNL is het niet duidelijk wat je als belangrijke of essentiële entiteit kunt doen om een openbaarmaking van een significant incident tegen te gaan, wanneer je vindt dat je daarvoor een gerechtvaardigd belang hebt.
- Tenslotte is het niet duidelijk wie (gevolg)schade herstelt wanneer deze ontstaat bij het openbaren van een incident van de betrokken entiteit.

- Artikel 65 Cbw gaat over vertrouwelijke gegevens en welke mogelijkheden de verschillende autoriteiten hebben om vertrouwelijke gegevens te verstrekken van een essentiële of belangrijke entiteit. Verschillende cybersecuritydienstverleners vallen straks onder de Cbw. Dat vindt CVNL een terechte ontwikkeling. Echter, cybersecuritydienstverleners hebben een vertrouwensrelatie met hun klanten. Het is dus voor CVNL en haar leden belangrijk dat vertrouwelijke gegevens van de entiteiten alleen betrekking hebben op de cybersecuritydienstverleners (als belangrijke entiteit) zelf en niet op de informatie die een cybersecuritydienstverlener in bezit heeft vanwege de diensten die worden verleend aan een klant.

- In paragraaf 9.4 Cbw staan vrijwillige meldingen beschreven. CVNL vindt dit een belangrijk stimulans om de weerbaarheid te vergroten en de drempel om te melden te verlagen. Echter, wij vinden het belangrijk dat wanneer een (vrijwillige) melding wordt doorgezet naar andere CSIRT's of andere relevante partijen de melder hiervan op de hoogte wordt gesteld.

Maatregelen

- Hoofdstuk 7 gaat over de Zorgplicht. In artikel 23 lid 1 en 2 staan de maatregelen beschreven die in lijn moeten zijn met de risico's:
  - CVNL is van mening dat de maatregelen om de toeleverancierskeketen te beschermen onvoldoende zijn uitgewerkt in lid 1.
  - In artikel 23.3 staat beschreven dat de entiteit ook de fysieke omgeving moet beschermen. CVNL vindt dit een goede zaak. Echter, wij pleiten vanuit deze all-hazard benadering dat ook de te maken risicoanalyses zich richten op het fysieke én digitale domein in een gecombineerde risicoanalyse.
  - Veel klanten van cybersecuritydienstverleners vragen aan onze leden (lees: de cybersecuritydienstverleners) welke passende en evenredige maatregelen moeten worden genomen om aan de verplichting in de Cbw te voldoen. Vanuit dat oogpunt vinden we dat artikel 23 te vrijblijvend is beschreven. Wij zouden graag zien dat in dit artikel de maatregelen zoals beschreven in artikel 21 lid 2 van de

NIS2 worden opgenomen om onduidelijkheid over de status van deze maatregelen te voorkomen.

- Het voldoen aan een eigen normenkader betekent op zichzelf niet dat een entiteit aan de zorgplicht van artikel 23 Cbw voldoet. CVNL is een sterk voorstander dat toezichthouders het gebruik van (inter)nationaal gehanteerde, van toepassing zijnde, normenkaders meenemen in de beoordeling van de toezichthouders met betrekking tot het voldoen aan de zorgplicht.
- CVNL adviseert dat de toezichthouders toewerken naar een geharmoniseerd normenkader(s).

- In artikel 32 Cbw staat beschreven:
  "1. Een essentiële of belangrijke entiteit stelt in voorkomend geval onverwijld de ontvangers van haar diensten in kennis van significante incidenten die een nadelige invloed kunnen hebben op de verlening van die diensten.
  2. De essentiële entiteit respectievelijk de belangrijke entiteit deelt de ontvangers van haar diensten, die mogelijkerwijs door een significante cyberdreiging in relatie tot het ontvangen van die diensten worden getroffen, onverwijld mee welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indien nodig stelt de entiteit die ontvangers ook in kennis van de desbetreffende significante cyberdreiging."
  CVNL vindt dit een zeer goede ontwikkeling die kan bijdragen aan meer openheid over incidenten en het vergroten van de weerbaarheid van een hele keten.
  - Echter, CVNL zet wel vraagtekens bij de effectiviteit van deze maatregelen omdat er geen nadere omschrijving wordt gegeven over welke kennis (lid 1) het gaat, dan wel wat wordt bedoeld met 'ontvangers' (lid 2):
    - Kennis: Dit zou meer moeten zijn dan de feitelijke constatering dat er een incident is, maar juist de aanwezige kennis die noodzakelijk is om de "ontvangers" te informeren zodat zij maatregelen kunnen treffen.
    - Ontvanger: Wat is de definitie van ontvanger? In de optiek van CVNL worden hiermee zowel de klanten als ook de toeleveranciers bedoeld.
  - Er zijn veel signalen gerelateerd aan cyberveiligheid waar entiteiten dagelijks mee te maken krijgen en het heeft geen zin om de ontvangers van de diensten over al deze signalen te informeren. Ontvangers van diensten moeten alleen worden geïnformeerd over significante incidenten wanneer zij hierdoor worden getroffen, en alleen in gevallen waarin zij specifieke maatregelen moeten nemen om de impact van dergelijke incidenten te beperken. Hier zou een afwegingskader om de significantie te bepalen kunnen helpen.

- In paragraaf 9.1 Cbw wordt de Meldplicht beschreven. In de optiek van CVNL kan de effectiviteit van een meldplicht alleen worden bereikt door goede monitoring van netwerkverkeer of andersoortige monitoringmaatregelen. Deze verplichting ontbreekt in zowel het wetsvoorstel als de MvT. We doen een dringende oproep om in een AMvB deze lacune alsnog in te vullen. Immers, nu kan een essentiële of belangrijke entiteit door het niet monitoren van het netwerkverkeer veel incidenten niet tijdig signaleren, stoppen of cyberdreigingen tegengaan.

- Een CSIRT krijgt verschillende taken vanuit de Cbw. Het is niet duidelijk wanneer een essentiële of belangrijke entiteit, wanneer deze niet naar behoren is geholpen of geadviseerd, een klacht over de bevoegde autoriteit kan indienen en bij wie.

Entiteiten

- Entiteiten die onder de CER vallen, vallen ook direct onder de Cbw. Het is echter vice versa onduidelijk waarom entiteiten die onder de Cbw vallen niet automatisch ook onder de CER vallen. Daarnaast zijn er organisaties die nu onder de Wbni vallen maar straks niet onder Cbw. Deze kunnen echter bij monde van de Minister wel aangewezen worden. Tenslotte heeft een vakdepartement nog de mogelijkheid om entiteiten aan te merken als zijnde essentieel of belangrijk. Onzes inziens gaat dit tot veel onduidelijkheid leiden. Geadviseerd wordt om in AMvB's meer duidelijkheid op dit onderwerp te bieden.

Toezicht

- In artikel 68 Cbw staat beschreven dat de bevoegde autoriteit een controlefunctionaris kan aanwijzen ten aanzien van een essentiële entiteit. CVNL herkent dat sommige entiteiten de noodzakelijke kennis ontberen die nodig is om een organisatie op een cyberveilige manier in te richten. Echter, wij pleiten ervoor dat de functieomschrijving van deze onafhankelijke adviseur nader wordt omschreven, bijvoorbeeld in een AMvB. Uiteraard willen we vanuit CVNL meedenken over de functie-eisen van zo'n onafhankelijke controleur.

- Toezicht van de CER is nog niet ingericht in het wetsvoorstel. CVNL is van mening dat het toezicht van zowel de CER als de Cbw voor een entiteit bij dezelfde toezichthouder moeten worden ondergebracht, mede ook vanwege de integratie van fysieke en digitale weerbaarheid/veiligheid.

- Wij missen in de Cbw, dan wel de MvT, een kader voor toezichthouders voor wat betreft de kwaliteit van het toezicht. Sommige toezichthouders hebben nog weinig ervaring met cybersecuritytoezicht. Het is dan ook belangrijk dat er een kader komt die hierin een baseline zet.

- In artikel 70 en 71 Cbw worden de gerichte en ad hoc beveiligingsaudit beschreven. CVNL vindt het een goede ontwikkeling dat de entiteit zowel de werking als het bestaan van maatregelen aantoonbaar moeten maken. Ook hierbij geldt dat we van mening zijn dat er nader te omschrijven eisen moeten komen aan de onafhankelijke deskundige om de kwaliteit van een beveiligingsaudit te kunnen garanderen.

- In de MvT is in hoofdstuk 7 de relatie tot nationale wetgeving beschreven. Hierin staat genoemd "*In deze paragraaf wordt beschreven welke verplichtingen er op grond van nationale wetgeving reeds gelden voor specifieke sectoren en wordt bezien hoe die verplichtingen zich verhouden tot de verplichtingen uit de NIS2-richtlijn. Daarbij wordt de wetgeving per ministerie bekeken.*"
  Entiteiten hebben te maken met nationale wetgeving en sectoraal toezicht. Daarbij geldt voor verschillende sectoren dat sectorale toezichthouders vergelijkbare eisen stellen aan de weerbaarheid van entiteiten en daarnaast entiteiten verplichten tot het doen van een melding conform sectorale wetgeving. Het is verstandig om de overlap duidelijk te maken tussen de Cbw en sectoraal toezicht als er afspraken tussen toezichthouders worden gemaakt omtrent "voorrang in geval van significant incident", normenkader, et cetera.

- De Cbw geeft de toezichthouders en CSIRT's verschillende mogelijkheden om te zorgen dat informatie over kwetsbaarheden, incidenten of dreigingen bij de juiste instanties terechtkomt. Echter, wij zouden graag in een AMvB opgenomen willen zien dat informatie van of over een entiteit door de bevoegde autoriteit altijd in eerste aanleg opgevraagd wordt bij de desbetreffende entiteit. Cybersecuritydienstverleners moeten verschoond worden van het delen van informatie over hun klanten met de bevoegde autoriteiten. Zij kunnen dit uiteraard wel delen na toestemming van de desbetreffende entiteit.

- De drempelwaardes om te melden moeten nog verder worden uitgewerkt in een AMvB. Echter, verschillende sectoren, zoals de cybersecuritysector, werken vaak land

overstijgend. CVNL pleit er dan ook voor om deze drempelwaardes verder uit te werken op Europees niveau en niet op nationaal niveau.

Bestuurder

- Artikel 26 Cbw gaat over de governance. Deze is wat CVNL betreft nog te onduidelijk en vrijblijvend beschreven. Wij pleiten voor het verder uitwerken van de kennis en vaardigheden van de bestuurder (lid 4) en de aantoonbaarheid van de kennis en vaardigheden middels een certificaat van deelname (lid 5). In lid 6 staat dat *"bij of krachtens AMvB regels kunnen worden gesteld over de training"*. CVNL pleit ervoor om het woord 'kunnen' te schrappen in dit artikel zodat deze wordt opgenomen in een AMvB.

- In artikel 26 Cbw lid 2.a staat beschreven dat een lid van het bestuur van een entiteit over de kennis en vaardigheden beschikt om *"risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren"*. CVNL is van mening dat het woord 'identificeren' op verschillende manieren kan worden geïnterpreteerd en verzoekt om dit woord aan te passen. Onze suggestie zou zijn 'waarnemen, beoordelen en sturen'.

- Vanwege de verschillende variaties in bestuur qua grootte, taakstelling, etc. is CVNL van mening dat artikel 26 lid 2 Cbw moeilijk uitvoerbaar is. Een andere toelichting in de verschillende AMvB's is wat ons betreft wenselijk.

Overig

- In artikel 1 van de concept Cbw wordt in de begripsbepaling een aantal in de concept wettekst aangehaalde begrippen verder toegelicht. Echter, deze begrippenlijst is naar onze mening niet volledig. CVNL mist een aantal essentiële begrippen in dit artikel, zoals 'cyberhygiëne' en 'bestuurder'.[1] CVNL vindt het jammer dat voor de definities niet wordt verwezen naar het breed in Nederland gehanteerde Cybersecuritywoordenboek (https://cyberveilignederland.nl/woordenboek).

- In artikel 15 lid c mist een spatie: 'deoverige'.

[1] CVNL is één van de initiatiefnemers van het Cybersecurity Woordenboek. Normaliter zou deze al een update hebben gekregen. Echter, vanwege het uitstellen van de internetconsultatie is gewacht met het aanpassen van het woordenboek. CVNL stelt voor om het woordenboek te gebruiken voor de begrippenlijst zoals gehanteerd in de Cbw voor wat betreft de woorden die zijn opgenomen in het woordenboek.

- In artikel 30 staat een spelfout: ‘Eem’.

- Artikel 39 lid b staat een spelfout. Hier staat tweemaal een ‘b’, waar dat een ‘b’ en een ‘c’ zou moeten zijn.

- Vanuit de Europese Unie zijn verschillende wetten en richtlijnen in ontwikkeling die een relatie hebben met de Cbw. In de Cbw staat er dan ook een aantal benoemd. Echter, er zijn ook enkele wetten en regels die nog niet gelden, dan wel het formele besluitvormingsproces nog niet hebben doorlopen. CVNL pleit ervoor dat de relatie van de Cbw met, bijvoorbeeld, de Cyber Resilience Act (CRA), Cyber Solidarity Act (CSA) en Radio Equipment Directive (RED) wel benoemd wordt in de nog uit te werken AMvB.

- In artikel 50, lid 3 en lid 5 staan spelfouten (“zij maen dat beleid” en domeinnaamregistratiediensten verlemen”).

- CVNL vindt het in de MvT gehanteerde aantal minuten die het een entiteit gaat kosten om een melding goed te kunnen afhandelen niet realistisch. In de MvT gaat men uit van 480 minuten dat het een entiteit gaat kosten om een melding te doen (8 uur), dat is inclusief de melding binnen 24 uur, de tussenrapportage en eindrapportage. De sector heeft veel ervaring met het helpen van het doen van meldingen aan toezichthouders en stelt vast dat dit niet realistisch is. Het uitvoeren van een goede melding vraagt, naar onze ervaring, meer tijd.
- De kostenindicatie van €60, zoals beschreven in de MvT is niet marktconform (te laag) en bovendien niet toekomst vast. CVNL stelt voor om duidelijk te maken wat een initiële melding minimaal inhoudt en daar een geharmoniseerd instrumentarium voor aan te bieden om zowel de kwaliteit van de melding te vergroten als de last voor entiteiten zo klein mogelijk te houden.

<u>Over Cyberveilig Nederland</u>

Cyberveilig Nederland (CVNL) is de belangenvereniging van de cybersecuritysector in Nederland. In die hoedanigheid maken we ons sterk voor het creëren van meer transparantie en kwaliteit in de markt. Zo zijn we betrokken bij diverse keurmerk ontwikkelingen vanuit het CCV[2], zijn we initiatiefnemer van het Cybersecurity

[2] https://hetccv.nl/keurmerken/cybersecurity/

Woordenboek[3] en maken we buyers guides om klanten van cybersecuritydienstverleners te helpen met het kiezen van de juiste diensten[4]. Ook behartigen we de belangen van de cybersecuritysector richting stakeholders zoals de overheid, wetenschap en politiek. Onze missie is de digitale weerbaarheid van Nederland te vergroten. Eén van de eisen om dit te bereiken is het actief delen van informatie. Vanuit CVNL stimuleren we dit door samen te werken met relevante overheidspartijen en andere belanghebbenden. In die hoedanigheid zijn we door het ministerie van Justitie en Veiligheid in 2020 aangewezen als schakelorganisatie onder de wet beveiliging netwerk informatiesystemen (Wbni)[5]. Daarnaast spelen we een actieve rol in het tot stand komen en verder ontwikkelen van het 'landelijk dekkend stelsel van informatieknooppunten'[6], zijn we vanaf de start betrokken bij het Anti Abuse Netwerk (AAN)[7], zijn we actief deelnemer in het Programma Cyclotron[8] en zijn we mede-initiatiefnemer van Project Melissa waar we (de gevolgen van) ransomware bestrijden[9].

[3] https://cyberveilignederland.nl/woordenboek
[4] https://cyberveilignederland.nl/werkgroepen#kwaliteit-transparantie
[5] https://www.ncsc.nl/actueel/nieuws/2020/december/9/intensievere-informatie-uitwisseling-ncsc-en-nederlandse-cybersecuritybedrijven
[6] https://www.nctv.nl/onderwerpen/landelijk-dekkend-stelsel
[7] https://www.abuse.nl/
[8] Cyclotron moet leiden tot een platform waarbinnen publieke en private partijen informatie delen over digitale incidenten en dreigingen. Zie: https://www.nctv.nl/onderwerpen/programma-cyclotron
[9] Project Melissa is een samenwerkingsverband tussen publieke en private partijen om ransomware aanvallen te bestrijden. Vanuit de overheid zijn het NCSC, OM en politie betrokken. Het gezamenlijke doel is om Nederland een onaantrekkelijk doelwit te maken voor ransomwarecriminelen. Zie: https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.pdf en https://cyberveilignederland.nl/actueel/cyberveilig-nl-politie-om-en-ncsc-werken-samen-aan-ransomwarebestrijding