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

info@cyberveilignederland.nl

www.cyberveilignederland.nl

KvK 71802525

Noordwijk, 28 maart 2025
Ref.: PA903-250328

Reactie Cyberveilig Nederland op het Cyberbeveiligingsbesluit (Cbb).

Geachte heer/mevrouw,

Cyberveilig Nederland (CVNL) heeft met veel belangstelling het concept Cyberbeveiligingsbesluit (Cbb) gelezen. De Cbb is de uitwerking van het voorstel van de Cyberbeveiligingswet (Cbw) die vorig jaar is voorgelegd in een openbare internetconsultatie en waar CVNL ook op heeft gereageerd.[1] De Cbw is de Nederlandse uitwerking van de Europese Network and Information Security Directive (NIS2-richtlijn). Het doel van de NIS2-richtlijn is '*om een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie te bereiken, teneinde de werking van de interne markt te verbeteren*. Dit wordt beoogt door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken.

CVNL staat zeer positief over de NIS2-richtlijn gezien het gegeven dat nog veel organisaties achterblijven met het nemen van maatregelen om hun eigen (digitale) weerbaarheid te vergroten, terwijl de dreigingen alleen maar zijn toegenomen. Ook de toenemende digitale afhankelijkheden waardoor een incident kan doorwerken in een (digitale) keten maakt de NIS2 naar onze mening noodzakelijk.

CVNL maakt graag gebruik van de mogelijkheid die wordt geboden om op de consultatie van het Cbb te reageren. Hierbij dient opgemerkt te worden dat de leden van CVNL zelf grotendeels niet onder de Cbb komen te vallen. Dat is enerzijds omdat het merendeel van de aangesloten cybersecurity bedrijven niet aan de jaaromzet en het aantal medewerkers komt.[2] Anderzijds omdat cybersecurity organisaties die wel als entiteit (digitale dienstverlener) onder de NIS2 komen te vallen zich moeten conformeren aan de Uitvoeringsverordening (EU) 2024/2690, waardoor de artikelen 6 t/m 16 en 24 van de Cbb niet voor hun van toepassing is. Vanuit CVNL reageren we dan ook in hoeverre cybersecurity bedrijven op grond van de Cbb hun klanten goed

[1] https://cyberveilignederland.nl/actueel/inbreng-cvnl-op-internetconsultatie-cyberbeveiligingswet-cbw
[2] https://ondernemersplein.kvk.nl/nis2-richtlijn-beschermt-netwerk-en-informatiesystemen-tegen-cyberbeveiligingsrisicos/

kunnen adviseren om aan de eisen van de Cbb (en de Ministeriële Regeling/MR) te voldoen. Hierbij zien we de volgende aandachtspunten:

1. **Risicogebaseerde aanpak komt onvoldoende naar voren**
2. **Administratieve lasten van (MKB)entiteiten zullen fors toenemen**
3. **Herzie de artikelen over eisen aan de trainingen bestuurders**
4. **Zorg snel voor meer duidelijkheid over complexe bedrijfsmodellen**
5. **De rol/taken van de CSIRT in het kader van Incidentmanagement moet duidelijker**
6. **Enkele generieke opmerkingen**
7. **Opmerking over advies Raad van State over Cbw: WOO**

1. Risicogebaseerde aanpak komt onvoldoende naar voren

CVNL is van mening dat de risicogebaseerde benadering die centraal staat in de NIS2-richtlijn onvoldoende in de Cbb verwerkt is. De Cbb is naar onze mening een 'compliancy' gedreven besluit omdat het grotendeels bestaat uit het opleggen van procedures, beleid en planvorming in de beschreven artikelen én een omschrijving waaruit deze dan moeten bestaan. Dit terwijl de risicogebaseerde benadering waar de NIS2 voor staat juist belangrijke en essentiele entiteiten in staat stelt en stimuleert om hun maatregelen af te stemmen op de specifieke risico's die voor hun entiteit van toepassing is. Cybersecurity bedrijven kunnen entiteiten dan beter adviseren en hun als *trusted advisor* helpen in het (laten nemen van) gerichte maatregelen afgestemd op hun specifieke risico's. De Cbb en de MR laten te weinig over aan het zelf kunnen invullen en regelen van de cyberweerbaarheid. De Cbb staat vol met voorschriften, terwijl het juist belangrijk is dat entiteiten de vrijheid moeten kunnen hebben om op basis van vooraf beschreven doelen, zelf invulling te geven aan het hoe. CVNL realiseert zich dat dit met name geldt voor volwassen cybersurity entiteiten en dat meer onvolwassen entiteiten deze 'guidence' wel waarderen. Onze suggestie is dan ook om de volgende suggesties mee te nemen in de Cbb:

- **Artikel 7 (beleid over risicomanagement)**
  De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over risicomanagement voor de beveiliging van haar netwerk- en informatiesystemen. De entiteit neemt op basis van dit beleid maatregelen om op een structurele wijze tot een beveiligingsniveau te komen dat is afgestemd op de risico's. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.

  Cyberveilig Nederland is van mening dat dit artikel aan waarde kan toenemen wanneer ook de eerste stap in je risicomanagement proces wordt opgenomen in dit artikel: identificatie. Entiteiten moeten hierbij identificeren:
  - wat de belangrijkste te beschermen zaken zijn
  - wat de grootste risico's, dreigingen en gevaren er zijn
  - welke actoren/factoren een rol spelen bij deze risico's/dreigingen/gevaren
  - welk risico appetite de organisatie heeft (vastgesteld door het management/bestuur)

- welk restrisico de organisatie acceptabel vindt (vastgesteld door het management/bestuur)
- welke stakeholders een rol spelen bij het mitigeren of uitbesteden van deze risico's, dreigingen of gevaren
- welke processen/welk beleid je gaat ontwikkelen om bovenstaande te controleren

- **Artikel 9 (bedrijfscontinuïteit en crisisbeheer)**
  Maak het testen en oefenen concreter door het laten toelichten voor welke periode (dag, maand, jaar) wordt gekozen, of voor welke vorm (zoals een Tabletop) en waarom en maak dit risicogebaseerd.
- **Artikel 15 (beveiligingsaspecten ten aanzien van toegangsbeleid)**
  CVNL vindt dat je fysieke en logische toegang uit elkaar moet trekken op basis van de risicobeoordeling die je maakt als entiteit. Omdat fysieke beveiliging van netwerk en informatiesystemen veelal wordt vergeten zou CVNL er voor pleiten om hier een apart artikel aan te wijden. Hier kan ook een link gemaakt worden met de WWKE (fysieke toegang).
- De specifieke uitdagingen van OT-security komen onvoldoende tot uiting in de Cbb en de MR. OT-security kent doorgaans andere uitdagingen en security oplossingen dan in IT-(netwerk)omgevingen gebruikelijk zijn. Monitoring van het netwerk, patchen van systemen of de levensduur van apparaten zijn enkele aandachtspunten. Expliciete verwijzingen naar standaarden zoals de IEC 62443, en een sectorspecifieke invulling van de zorgplicht helpen hierbij.

2. Administratieve lasten van (MKB)entiteiten zullen fors toenemen

Vanwege de hierboven beschreven 'compliancy-insteek' van de Cbb zal de administratieve lasten van organisaties sterk toenemen, zonder dat het daadwerkelijk een positieve impact zal hebben op de daadwerkelijke vergroting van de weerbaarheid van deze organisaties. Het voldoen aan de Cbb (en de MR) zal een grotendeels papieren exercitie worden waarbij een hoeveelheid aan beleidsdocumenten, procedures en andere documenten worden gevraagd. Daarnaast wordt in de Cbb op diverse punten een scheiding van rollen gevraagd terwijl dat voor met name middelgrote entiteiten zal betekenen dat zij extra personeel moeten werven of extern aantrekken terwijl de meerwaarde van die scheiding van functies onvoldoende wordt gemotiveerd. Voorbeelden hiervan zijn:

- **Artikel 6. (beleid over beveiliging van netwerk- en informatiesystemen)**
  In het kader van het beleid, bedoeld in het eerste lid, stelt de essentiële entiteit of belangrijke entiteit de rollen, verantwoordelijkheden en bevoegdheden in relatie tot de beveiliging van haar netwerk- en informatiesystemen vast. De entiteit zorgt ervoor dat conflicterende rollen, verantwoordelijkheden en bevoegdheden gescheiden worden.
  CVNL vraagt zich af of dit bij middelgrote organisaties uitvoerbaar is omdat dit soort organisaties vaak niet veel (eigen) personeel in dienst heeft. Daarnaast vraagt CVNL zich af wat ' gescheiden' moet worden, omdat sommige rollen, verantwoordelijkheden en bevoegdheden vaak prima in één functie kan bestaan. Tenslotte zijn we van mening dat er andere mogelijkheden voor compenserende maatregelen rondom de

risicogebaseerde aanpak. Denk maatregelen bijvoorbeeld aan striktere monitoring/controle of taakroulatie.

- **Artikel 10 (beveiliging van de toeleveringsketen)**
  CVNL is van mening dat de auditlast door dit artikel enorm zal toenemen. Elke essentiele en belangrijke entiteit zal bewijslast gaan eisen van de toeleveranciers. We snappen dat hier voor directe toeleveranciers en dienstverleners is gekozen (zie ook DORA). Echter bij DORA wordt onderscheid gemaakt tussen materiële en niet-materiële (sub)contractors, op het niveau van functie voor de prestatie die geleverd moet worden. Overweeg de CBB te laten aansluiten bij het in de DORA gehanteerde onderscheid: Dat kan door te benoemen dat enkel de kritieke en belangrijke functies die een toeleverancier levert en een materiële bijdrage leveren aan de prestatie in scope zijn. Daarnaast is het daardoor mee in lijn met de risicogebaseerde aanpak
  Concreet:
    - In lid 3 staat dat je los van het contract ook nog je afspraken schriftelijk moet vastleggen. Waarom?
    - Maak bij dit artikel duidelijk dat het hier om toeleveranciers gaat die een directe impact kunnen hebben op je bedrijfsvoering en niet om de bakker om de hoek of de leverancier van koffieautomaten.

- **Artikel 11 (beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen)**
  Maak in dit artikel een koppeling met de Cyber Resilience Act (CRA)/Verordening Cyberweerbaarheid die straks bindende eisen gaat stellen aan de cyberveiligheid van digitale producten. Entiteiten moeten controleren of leveranciers de juiste waarborgen heeft maar niet zelf de eisen voor haar producten ontwikkelen, want dat zal zorgen voor enorme (onnodige) administratieve lastendruk. Dat laatste vindt op Europees niveau plaats, op basis van de CRA.

- **Artikel 12 ((basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging)**
  In dit artikel wordt gesproken over opleiding en niet training zoals in de artikelen vanaf 22. Training is een logischer term dan opleiding want de laatste suggereert veel tijd en inspanning wat niet altijd nodig is voor de doelgroep/medewerkers voor wie het bedoeld is. Dit brengt onbedoeld extra lasten met zich mee.

Cyberveilig Nederland is verder van mening dat de toepassing van de door het CCV uitgebrachte keurmerken die reeds bestaan of nog in ontwikkeling zijn actief omarmt zou moeten worden door de overheid in de Cbb en de MR. Deze zijn essentieel om entiteiten te helpen een vertrouwde cybersecurity partner te vinden die een entiteit kan helpen met het voldoen aan de wet. Hierbij is het wel noodzakelijk dat de keurmerken worden doorontwikkeld en gestimuleerd worden vanuit de overheid en de betrokken stakeholders, waaronder CVNL zelf.

Tenslotte vraagt CVNL om het toezicht en handhaving zo veel mogelijk af te stemmen onder de verschillende toezichthouders. En dan niet alleen gericht op toezicht op deze wet maar ook op andere sectorale wetgeving die cybersecurity in hun toezicht- en handhavingstaken hebben. Dat zal de toezichtlasten voor entiteiten niet alleen beperken, maar geeft ook voordelen voor entiteiten die onder verschillende toezichthouders komen te vallen.

3. Herzie de artikelen over eisen aan de trainingen bestuurders

CVNL vindt het een zeer goede ontwikkeling dat de NIS2/Cbw de verantwoordelijkheid van cybersecurity neerlegt waar deze thuis hoort: bij de bestuurder. In artikel 24 van de NIS2 staat dan ook: *Voorts moedigen de lidstaten essentiële en belangrijke entiteiten aan om gebruik te maken van gekwalificeerde vertrouwensdiensten*. In zowel de Cyberbeveiligingswet, het Cyberbeveiligingsbesluit en de Cyberbeveiligingsregeling wordt vervolgens niet ingegaan hoe essentiële en belangrijke entiteiten gekwalificeerde vertrouwensdiensten kunnen inzetten om invulling te geven aan hun zorgplicht met betrekking tot cyberbeveiliging:

Echter **Artikel 20 (doel van de training)** wordt ons inziens onvoldoende de doelstelling van de training uitgewerkt. Een verwijzing naar de Artikelen 6 tot en met 10 in relatie tot de training van bestuurders kan hierbij helpen omdat de training zich zou moeten focussen op (strategisch) risicomanagement, incidentmanagement en ketenafhankelijkheden.
Daarnaast is CVNL van mening dat de in **Artikel 22 (eisen aan de trainer)** beschreven eisen aan de trainer verder gaat dan de NIS2 voorschrijft omdat er een onafhankelijke externe trainer wordt gevraagd. Veel organisaties (die al over een groter volwassenheidsniveau beschikken) hebben vaak voldoende security experts in dienst die een meer op de entiteit gerichte training kunnen verzorgen dan een externe partij. Ook vanuit de positionering van deze experts richting de bestuurder is CVNL van mening dat deze mogelijkheid expliciet geboden moet worden in de Cbb.
Tenslotte vraagt CVNL om in **Artikel 23 (eisen aan het certificaat)** een aantal eisen te schrappen, zoals de taal en het aantal uren dat de training is gevolgd.

4. Zorg snel voor meer duidelijkheid over complexe bedrijfsmodellen

De leden van CVNL krijgen veel vragen van hun klanten over complexe bedrijfsstructuren en wat dat betekent voor het wel/niet vallend onder de Cbw/NIS2. De registratie zoals die is beschreven in **artikel 28** (**(verstrekking overige informatie)** is hierin niet eenduidig. Voorbeelden van organisaties met meerdere BV's onder één holding, of van meerdere BV's die binnen verschillende sectoren of in verschillende landen zijn gevestigd zijn enkele voorbeelden. CVNL vraagt zich af in hoeverre het gebruik van MijnNCSC en in het verlengde hiervan (voor de registratie van MijnNCSC) het gebruik van e-herkenning toegepast moet worden. CVNL denkt dat er mogelijkheden zou moeten komen van een 'groepsregistratie' waarbij verbonden rechtspersonen binnen één concern zich als groep kunnen registreren, met één centrale contactpersoon voor meldingen.

5. De rol/taken van de CSIRT in het kader van Incidentmanagement moet duidelijker

In de **Nota van toelichting, betreffende 2.4: Aanwijzing CSIRT en coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden,** wordt in Artikel 16, eerste lid, Cbw bepaald *dat voor alle essentiële entiteiten en belangrijke entiteiten bij of krachtens algemene maatregel van bestuur een Computer security incident response team (hierna: CSIRT) wordt aangewezen. Het CSIRT heeft op grond van artikel 16, derde lid, Cbw, onder meer tot taak om genoemde entiteiten in geval van dreigingen, kwetsbaarheden en incidenten vroegtijdig te waarschuwen en bijstand te verlenen.* In artikel 2 Cbb wordt geregeld welke partij voor essentiële entiteiten en belangrijke entiteiten als CSIRT wordt of kan worden aangewezen. Voor een toelichting hierop wordt verwezen naar de artikelsgewijze toelichting op deze bepaling.

CVNL heeft van verschillende van onze leden signalen ontvangen dat verschillende entiteiten die straks onder de Cbw vallen voornemers zijn om hun contracten met Incident Respons-partijen op te zeggen omdat zij van mening zijn dat het betrokken CSIRT de taken van een IR-partij gaat overnemen. CVNL vraagt dan ook duidelijkheid waar de bijstand die het NCSC (of een andere CSIRT) uit zal bestaan in geval van een incident of crisis.

6. Enkele generieke opmerkingen:

- CVNL pleit voor het veranderen van het woord “binnen” in “bij”. Binnen suggereert een fysieke aanwezigheid terwijl met hybride werk-mogelijkheden ook in letterlijke zin buiten de entiteit kan plaatsvinden. Voorbeelden zijn artikel 6,
- Zorg ervoor dat de eisen uit EU-uitvoeringsverordening (voor de digitale sector) worden overgenomen in het Cbb en de MR, danwel minimaal met elkaar in lijn zijn, danwel dat wordt toegelicht hoe deze zich tot elkaar verhouden.
- In **Artikel 8 (Incidentenbehandeling)** lijken Incidenten en vulnerability management door elkaar heen te lopen.
- In **Artikel 8 (Incidentenbehandeling)** missen we het onderzoek naar oorzaken van een (significant) incident. Vaak zijn oorzaken bij een incident namelijk niet door een entiteit zelf weg te nemen, waardoor dit onderzoek belangrijk is in het kader van ketenafhankelijkheden en het doorwerken van incidenten in de keten.
- In **Artikel 9 (bedrijfscontinuïteit en crisisbeheer)** zou het niet alleen maar om de betrouwbaarheid van back-ups moeten gaan, maar ook om de beschikbaarheid en integriteit.
- In **Artikel 9 (bedrijfscontinuïteit en crisisbeheer)** over (beveiligde) noodcommunicatie bij crisissen. Bij een crisis is noodcommunicatie noodzakelijk. Uiteraard bij voorkeur ook beveiligd, maar communicatie gaat bij een crisis voor beveiliging. CVNL verzoekt een aangepaste formulering van dit artikel.
- In **Artikel 10 (beveiliging van de toeleveringsketen)** wordt er gesproken van “waar mogelijk”. Slaat dit op de schriftelijke afspraken die je “mogelijk” kan maken of slaat het op het maken van “afspraken indien mogelijk”?

- **Artikel 16 (beveiligingsaspecten ten aanzien van beheer van assets)** lijkt te gaan over Access Management, want er wordt gesproken over “logische toegang”. Waarom wordt dit dan niet zo benoemd, aangezien dit een veelvoorkomende en herkenbare term is in de cybersecurity?
- **Artikel 16 (beveiligingsaspecten ten aanzien van beheer van assets).** Asset beheer is nodig dat wanneer er een incident is te weten wat je assets zijn zodat de impact van een incident zo klein mogelijk is/wordt. CVNL mist in dit artikel dan ook de link naar de artikelen over incidentmanagement.
- **Artikel 16 (beveiligingsaspecten ten aanzien van beheer van assets), lid 2.** Deze classificatie dient ook te gelden voor de opgeslagen data (informatie); immers data of informatie is de asset die dient uiteindelijk beschermd te worden. Dit staat in punt 3 wel genoemd.
- In **Artikel 17 (attenderingen, adviezen en informatie)** vinden we de scope van de genoemde partijen te smal. CVNL is van mening dat de scope van genoemde partijen te smal. Meldingen van bijvoorbeeld organisaties als de DIVD zou ook onderdeel moeten zijn van dit artikel.

7. Opmerking over advies Raad van State over Cbw: WOO

In het advies van de Raad van State (RvS) omtrent de Cyberbeveiligingswet[3] vraagt de RvS een nadere motivatie waarom een afwijking, gezien de beperkingen in de Woo op de Cbw gerechtvaardigd is. CVNL is van mening dat transparantie belangrijk is binnen het werkveld van cybersecurity. Echter in deze is CVNL het nadrukkelijk eens met de opstellers van de Cbw dat entiteiten die informatie delen in het kader van de Cbw gevrijwaard moeten blijven van Woo verzoeken. Het delen van (gevoelige) informatie over incidenten moet worden gestimuleerd om van elkaars incidenten te kunnen leren en mogelijke patronen te kunnen onderkennen van de actoren. Entiteiten moeten er op kunnen vertrouwen dat deze informatie niet bij vanuit Woo-verzoeken bij derden terecht komt. Dit is momenteel verankerd in de voorganger van de Cbw, de Wbni en moet ook in de Cbw blijven om de weerbaarheid van Nederland te kunnen vergroten.

[3] https://www.raadvanstate.nl/adviezen/@147382/w16-24-00336-ii/#highlight=cybersecurity