Aanbevelingen voor de wetsbehandelingen (Wwke & Cbw)

De Wet weerbaarheid kritieke entiteiten (Wwke) en de Cyberbeveiligingswet (Cbw) vormen samen de ruggengraat van het Nederlandse stelsel voor digitale en fysieke veiligheid.

De cybersecuritysector, bij monde van Cyberveilig Nederland (CVNL), ziet in de huidige wetsvoorstellen belangrijke kansen, maar ook risico's die de werking van het stelsel kunnen verzwakken. Zie hieronder de belangrijkste punten, mede met input van onze leden.

1. Maak sancties op de zorgplicht constructief en risicoreducerend

De zorgplicht is een belangrijk instrument, maar zonder stimulans tot naleving blijft deze vrijblijvend. Toezichthouders kunnen sancties opleggen, maar deze hebben nu vooral een bestraffend karakter.

Voorstel vanuit de sector:
Laat een deel van de sanctie *verplicht* terugvloeien naar maatregelen die de weerbaarheid van de betreffende organisatie verhogen. Dit zorgt voor:

- directe risicoreductie
- een eerlijker speelveld
- een stelsel dat corrigerend én preventief werkt

2. Artikel 18 Cyberbeveiligingsbesluit: procedureel borgen, inhoudelijk verduidelijken

Hoewel artikel 18 niet in deze behandeling zit, is het belangrijk dat Kamerleden de context begrijpen. De sector ondersteunt de voorgestelde **voorhangprocedure** van VNO-NCW en FME.

Bezwaren richten zich op:

- De plek van het artikel: een ingrijpende last-resortmaatregel hoort niet onder een AMvB of onder de zorgplicht.
- Onvoldoende uitgewerkt proces: onduidelijkheid over informatievoorziening, uitvoerbaarheid en proportionaliteit.
- Cruciale rol van de toezichthouder: uitfaseren kan in sommige situaties juist een onveiliger situatie creëren.

3. Voorkom versnippering van toezicht – één herkenbaar en krachtig stelsel

Organisaties ervaren nu al onduidelijkheid over wie toezicht houdt, wanneer en met welke consequenties. Dit geldt voor Cbw, AVG én sectoraal toezicht.

Versnippering leidt tot:

- Inefficiëntie bij toezichthouders
- Onzekerheid bij organisaties
- Ongelijk speelveld tussen bedrijven
- Vertraagde risicoreductie

Een eenduidig, zichtbaar en krachtig toezichtstelsel is daarom essentieel. Dat betekent: duidelijke rolverdeling, herkenbare aanspreekpunten, en een toezichtstrategie die voor alle sectoren begrijpelijk en voorspelbaar is.

4. **Verminder complexiteit en overlap tussen wetten**

Organisaties worstelen met overlappende en soms tegenstrijdige verplichtingen uit:

- NIS2 / Cbw
- CRA
- DORA
- AVG
- Sectorale kaders

Vooral complexe organisaties raken hierdoor het overzicht kwijt. De sector pleit voor:

- Harmonisatie van definities, verplichtingen en processen
- Heldere guidance vanuit de overheid
- Centrale informatievoorziening in plaats van versnipperde documenten en interpretaties

5. **Harmoniseer meldplichten – voorkom dat rapportage een nalevingsoefening wordt**

Organisaties worden geconfronteerd met overlappende meldregimes (CRA, NIS2, DORA, AVG). Dit belast incidentrespons en leidt tot administratieve druk zonder veiligheidswinst.

De sector pleit voor:

- Één nationaal single front door voor meldingen
- Één geïntegreerd proces dat rapportage koppelt aan daadwerkelijke risicoreductie
- Met waarborgen dat meldingen enkel op de daarvoor bestemde plek terecht komen (vb vrijwillige meldingen onder Cbw enkel bij het NCSC en niet bij de toezichthouder)

6. **Borg capaciteit en expertise bij toezichthouders en aangemelde instanties**

De implementatie van nieuwe wetgeving staat of valt met voldoende capaciteit en expertise.

Nodig is:

- Structurele investering in vaardigheden en capaciteit
- Een toezichtcultuur die samenwerkingsgericht is in plaats van primair bestraffend
- Duidelijke verwachtingen richting marktpartijen
- Een toezichthouder die adequaat handhaaft

7. **Betrek de securitysector structureel bij normontwikkeling en uitvoering**

De overheid kan het gat in capaciteit en expertise niet alleen dichten. Minder volwassen organisaties evenmin.

Daarom is nodig:

- Structurele samenwerking met de securitysector bij het ontwikkelen van:
  - Keurmerken
  - Standaarden
  - Normenkaders
- Vroegtijdige betrokkenheid van de sector bij beleidsontwikkeling
- Benutten van marktcapaciteit in toezicht, certificering en ondersteuning

8. Redactionele correctie in artikel 8 lid 1 onderdeel f Cbw: vervang “drempel” door “plafond”

Cyberveilig Nederland adviseert een noodzakelijke redactionele wijziging in “artikel 8, lid 1, onderdeel f” van de Cyberbeveiligingswet. Het woord “drempel” moet worden vervangen door “plafond”.

Het verschil is juridisch en praktisch zeer relevant:

- Drempel overschrijden = boven de *ondergrens* uitkomen → een onderneming is *ten minste* middelgroot.
- Plafond overschrijden = boven de *bovengrens* uitkomen → een onderneming is *groter dan middelgroot*.

Met de huidige tekst worden middelgrote ondernemingen ten onrechte als essentieel aangemerkt, terwijl de regering in de Memorie van Toelichting duidelijk maakt dat dit alleen geldt voor ondernemingen groter dan middelgroot.

Onderbouwing vanuit de wet en toelichting

- De NIS2-richtlijn gebruikt expliciet de formulering “plafonds voor middelgrote ondernemingen overschrijden”.
- Paragraaf 5.1.1. van de Memorie van Toelichting bevestigt dat het gaat om ondernemingen die het plafond overschrijden.
- Als “drempel” blijft staan, ontstaat strijdigheid met artikel 12 lid 1 onderdeel a Cbw, dat middelgrote ondernemingen juist als belangrijk kwalificeert.

Vooruitblik op EU-wijzigingen

De Europese Commissie heeft op 20 januari 2026 een voorstel gepubliceerd (COM(2026) 13 final) dat de omvangsclassificatie opnieuw wijzigt. In dat voorstel worden essentiële entiteiten gedefinieerd als entiteiten die “exceed the ceilings for small mid-cap enterprises” zoals gedefinieerd in Aanbeveling (EU) 2025/1099.

Het is daarom des te belangrijker dat de Nederlandse wet nu al terminologisch correct is, zodat toekomstige implementatie soepel kan verlopen.