Reactie Internetconsultatie

Concept-Cyberbeveiligingswet

Transport en Logistiek Nederland (TLN) heeft kennis genomen van de concept-Cyberbeveiligingswet (Cbw), waarin de Europese NIS2-richtlijn in Nederland wordt geïmplementeerd. Wij maken graag gebruik van de mogelijkheid hierop te reageren.

Bij TLN zijn ruim 4.500 bedrijven aangesloten dit actief zijn in het beroepsgoederenvervoer over de weg en logistieke dienstverlening. Diverse van onze leden zullen te maken krijgen met de Cbw, hetzij direct als 'belangrijke' entiteiten, hetzij indirect als toeleverancier voor een essentiële of belangrijke entiteit.

TLN steunt het doel van de Richtlijn en de Cbw, namelijk het verhogen van de digitale veiligheid en weerbaarheid van bedrijven en organisaties die belangrijk zijn voor het functioneren van de economie en de samenleving. Voor ons is daarbij wel belangrijk dat:

- het voor organisaties en bedrijven helder is of zij wel of niet onder de Cbw vallen;
- de verplichtingen dusdanig zijn dat alle bedrijven ermee uit de voeten kunnen, ofwel dat de verplichtingen helder en proportioneel zijn.

Op deze punten hebben we ten aanzien van de concept-wettekst en memorie van toelichting een aantal zorgen. Dat komt mede omdat veel details nog in andere regelgeving – zoals een AMvB – nader moeten worden uitgewerkt. Onze belangrijkste zorgpunten zijn:

1. Het is voor diverse van onze leden nog onduidelijk of ze wel of niet onder de Cbw vallen. Transporteurs en logistiek dienstverleners leveren hun diensten vaak aan bedrijven in diverse andere sectoren. Zo zijn er bedrijven die zowel tuinbouwproducten ('levensmiddelen') als sierteeltproducten vervoeren. Of bedrijven die zowel horecabedrijven, als andere non-food detailhandelsbedrijven bevoorraden. Sommige activiteiten – en dus een deel van de omzet - vallen dan onder Bijlage 2 (Belangrijkste entiteiten), en andere activiteiten weer niet. Hoe moet in zo'n situatie worden omgegaan met het criterium dat de werkingssfeer is gericht op een 'middelgrote onderneming'?;
2. De onduidelijkheid over wel of niet een 'Cbw-entiteit' te zijn geldt ook voor Nederlandse onderdelen van internationale concerns (EU, of niet-EU). Daarnaast is voor deze bedrijven ook niet duidelijk bij welke toezichthouder incidenten die netwerk-breed doorwerken moeten worden gemeld en waar precies de aansprakelijkheid en de zorgplicht ligt.
3. De zorgplicht strekt zich voor bedrijven die rechtstreeks onder de Cbw vallen uit tot hun toeleveranciers. Dat zijn veelal mkb-bedrijven. Hoe kan worden voorkomen dat de eisen die aan toeleveranciers worden gesteld proportioneel en risicogericht zijn en dat de administratieve lasten beperkt blijven? En dat ook nog in de veelvoorkomende situatie waarin mkb-transportbedrijven onderdeel zijn van de toeleveringsketens van verschillende klanten die onder de NIS2-Richtlijn vallen uit verschillende landen?
4. In de MvT staat aangegeven dat Nederland naar verwachting gebruik gaat maken van de mogelijkheid om in een AMvB bepalingen vast te stellen die een hoger

cyberbeveiligingsniveau waarborgen. Dit lijkt ons een ‘nationale kop’, waarvan wij ons afvragen hoe die zich verhoudt tot het Hoofdlijnenakkoord 2024 – 2028 van het nieuwe kabinet. Het opleggen van aanvullende eisen vanuit Nederland creëert een ongelijk speelveld, en is voor bedrijven die in meerdere lidstaten opereren onwerkbaar.

Wij hopen dat bij de nadere uitwerking van de regelgeving op bovenstaande punten meer duidelijkheid wordt gegeven.

Zoetermeer, 1 juli 2024 (PP)