Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

Betreft: Reactie NLdigital op internetconsultatie Cyberbeveiligingsbesluit en Ministeriële Regeling
Plaats: Breukelen
Datum: 25 maart 2025

Geachte heer/mevrouw,

NLdigital is de brancheverenigingvan de digitale sector in Nederland. Onze achterban bestaat uit IT-leveranciers variërend van kleine IT-dienstverleners tot grote multinationals met zeer uiteenlopende producten en diensten. Onze leden krijgen op verschillende manieren te maken met NIS2: velen vallen direct onder de reikwijdte van de wet als digitale dienstverlener, terwijl anderen als IT-leverancier aan NIS2-entiteiten indirect te maken krijgen met de doorvertaling van de eisen naar hun dienstverlening. Door deze dubbelrol kijken wij niet alleen naar de directe impact van de eisen op de sector zelf, maar ook naar de doorvertaling die de klanten van onze leden naar hen moeten gaan doen.

Op basis van analyse van het voorgestelde Cyberbeveiligingsbesluit (Cbb) en de bijbehorende Ministeriële Regeling, hebben wij de volgende aandachtspunten die allen voorzien zijn van concrete aanbevelingen:

1. Streef harmonisatie van technische eisen na
2. Geen Nederlandse kop op trainingseisen voor bestuurders
3. Werkbare meldplichten in ICT-ketens
4. Gestandaardiseerde dienstverlening moet mogelijk blijven
5. Duidelijkheid voor verbonden rechtspersonen
6. Bewaartermijnen persoonsgegevens

1. Streef harmonisatie van technische eisen na

We constateren dat de verplichtingen voor entiteiten in de digitale sectoren direct voortvloeien uit de Europese Uitvoeringsverordening (EU) 2024/2690, terwijl de verplichtingen voor andere sectoren worden uitgewerkt in nationale ministeriële regelingen. Deze verschillende bronnen van regelgeving dreigen tot inconsistente implementatie-eisen te leiden, wat bijzonder problematisch is voor IT-leveranciers die diensten leveren aan meerdere sectoren.

NLdigital pleit voor maximale harmonisatie tussen de eisen in ministeriële regelingen onder het Cyberbeveiligingsbesluit en de Uitvoeringsverordening voor digitale sectoren. Zonder harmonisatie moeten onze leden per sector verschillende technische oplossingen implementeren voor dezelfde functionaliteiten zoals logging of back-ups. Dit verhoogt de kosten aanzienlijk, vergroot de technische complexiteit en verhindert schaalvoordelen. Dergelijke effecten zijn vooral een hogere Nederlandse regeldruk zonder enige winst op cybersecurityvlak. We stellen al vast dat de concept Ministeriële Regeling van EZ, LVVN, IenW en KGG op

meerdere punten afwijkende woordkeus heeft zonder te expliciteren of hier een afwijking bedoeld is of dat de intentie hetzelfde is.

NLdigital onderstreept dat effectieve beveiliging zowel binnen organisaties als in de toeleveringsketen niet alleen een kwestie is van documentatie en contractuele afspraken, maar vooral van operationele uitvoering en continue aandacht. Wij vragen dat de regelgeving en het toezicht hierop voldoende ruimte bieden aan organisaties om zelf invulling te geven aan deze operationele aspecten, passend bij hun bedrijfsmodel en risicoprofiel.

Concreet adviseren wij:

- Vul Artikel 19 Cbb aan met het uitgangspunt dat ministeriële regelingen hun implementatie moeten laten aansluiten bij Europese Uitvoeringsverordening (EU) 2024/2690. Hierbij zal op basis van risico-afwegingen per sector sprake zijn van lichtere of zwaardere vereisten. Wij pleiten ervoor om zoveel mogelijk dezelfde woordkeus na te streven waarbij alleen met expliciete toelichting hogere of andere eisen gesteld worden.
- Leg vast dat maatregelen van leveranciers die aantoonbaar voldoen aan de Uitvoeringsverordening, automatisch ook voldoen aan de sectorale eisen op die specifieke technische punten, tenzij er expliciet van afgeweken is.
- Breng de Ministeriële Regeling van EZ, LVVN, IenW en KGG hier mee in lijn.
- Bevorder dat toezichthouders bij de handhaving een geharmoniseerde benadering hanteren die aansluit bij de Europese kaders, en stimuleer dat nationale toezichthouders samenwerken met ENISA en de NIS Cooperation Group om interpretatieverschillen te minimaliseren - niet via extra regels, maar via gecoördineerde toezichtspraktijken die toezien op de effectiviteit in operationele uitvoering.

2. Geen Nederlandse kop op trainingseisen voor bestuurders

De eis dat bestuurderstrainingen door een onafhankelijke externe trainer gegeven moeten worden (artikel 22 Cbb), gaat verder dan de NIS2 voorschrijft en werkt contraproductief voor digitale bedrijven. In onze sector beschikken veel bestuurders al over diepgaande cybersecurity expertise, of zijn er interne experts die een effectievere en meer contextspecifieke training kunnen verzorgen dan een externe partij. NLdigital vraagt om flexibiliteit hierin, waarbij de focus ligt op het doel (adequate kennis) in plaats van het middel (externe training).

Concreet adviseren wij:

- Laat de eisen aan de trainer (artikel 22 Cbb) vervallen, zodat trainingen ook intern gegeven kunnen worden.
- Toets alleen dat de bestuurder na de training de vereiste kennis heeft.
- Houd de training vorm-vrij zodat deze toegespitst kan zijn op het bestaande kennisniveau van de bestuurder.

3. Werkbare meldplichten in ICT-ketens

NLdigital vraagt bijzondere aandacht voor de praktische uitvoerbaarheid van meldplichten in complexe ketens. IT-leveranciers bevinden zich in een unieke positie tijdens incidenten: zij moeten zelf melden, moeten hun klanten ondersteunen bij hun meldplicht, én moeten tegelijkertijd het incident oplossen. Daarnaast zien we dat ook complex samengestelde bedrijven voor meerdere entiteiten binnen hun organisatie moeten melden. Dit stelt hen voor dezelfde uitdaging

Bij grootschalige incidenten kan dit leiden tot een veelvoud aan parallelle meldplichten die waardevolle capaciteit weghalen van het daadwerkelijk oplossen van het probleem. Wij vragen de wetgever na te denken bij de uitwerking van meldplicht om dit proces overzichtelijk en doenbaar te houden voor dit soort situaties, zodat er niet onnodig afgeleid wordt van waar het om zou moeten gaan: het oplossen van het incident.

Concreet adviseren wij:

- Creëer een mechanisme voor 'gecoördineerde meldingen' waarbij een IT-leverancier bij grootschalige incidenten één centrale melding kan doen bij het CSIRT, die vervolgens doorwerkt naar de meldplichten van afnemers.
- Bied duidelijke handvatten voor de prioritering van activiteiten tijdens een incident, waarbij de nadruk in de acute fase ligt op het beperken van de impact.

4. Gestandaardiseerde dienstverlening moet mogelijk blijven

Het Cbb en de ministeriële regeling lijken op verschillende plaatsen uit te gaan van individuele afspraken tussen leveranciers en afnemers, wat niet past bij het schaalbare bedrijfsmodel van sommige digitale dienstverleners. In het bijzonder artikel 10, tweede lid van het Cbb en artikel 6 van de ministeriële regeling zouden kunnen worden geïnterpreteerd als vereiste voor maatwerkafspraken per klant.

Bij sommige vormen van IT-dienstverlening wordt gewerkt met gestandaardiseerde diensten die door veel afnemers worden gebruikt onder dezelfde voorwaarden (denk aan cloud-platforms, SaaS-oplossingen, etc.). Het zou de kosten en complexiteit van deze diensten enorm verhogen wanneer elke afnemer aparte cyberbeveiligingsafspraken moet maken die afwijken van de standaarddienst. Dit is onwerkbaar en economisch onhaalbaar voor veel van deze dienstverleners en hun afnemers. Daarbij leidt verhogen van complexiteit ook eerder tot minder veiligheid dan meer.

Concreet adviseren wij:

- Verduidelijk in artikel 10 Cbb en artikel 6 van de ministeriële regeling, of in de toelichting daarop, dat gestandaardiseerde cyberbeveiligingsafspraken voor one-to-many diensten volstaan, mits deze adequaat de veiligheidseisen voor de afnemer afdekken.
- Voorzie in een expliciete erkenning dat standaard leveringsvoorwaarden en serviceovereenkomsten kunnen voldoen aan de vereisten, zolang deze duidelijk de geleverde diensten en maatregelen ten behoeve van cybersecurity vastleggen.

5. Duidelijkheid voor verbonden rechtspersonen

De registratieverplichtingen in artikel 28 Cbb roepen bij leden vragen op voor groepen van verbonden rechtspersonen. Het is hen nog onduidelijk hoe organisaties met meerdere BV's onder één holding zich moeten registreren en meldingen moeten doen. Wij merken dat de werking van MijnNCSC en het gebruik van e-herkenning in deze context nog de nodige vragen oproept, met name in complexere bedrijven.

Concreet adviseren wij:

- Verduidelijk in artikel 28 of binnen een groep van verbonden rechtspersonen elke entiteit zich apart moet registreren, of dat een centrale registratie mogelijk is.

- Overweeg een mechanisme voor 'groepsregistratie' waarbij verbonden rechtspersonen binnen één concern zich als groep kunnen registreren, met één centrale contactpersoon voor meldingen.
- Besteed extra aandacht aan goede stap-voor-stap online toelichting op deze registratieprocessen.

6. Bewaartermijnen persoonsgegevens

De maximale bewaartermijnen voor persoonsgegevens in artikel 30 Cbb riep bij privacy-experts uit onze achterban veel vragen op: in lid 3 mogen deze tot 120 maanden voor toezicht doeleinden bewaard worden. Dat is extreem lang en roept vragen op over de proportionaliteit.

Concreet adviseren wij:

- Leg in de wet vast dat het overschrijden van de 60 maanden naar 120 maanden alleen gebeurd voor de casus die beschreven is in de Nota van Toelichting: bij lopende onderzoeken. Een dergelijke verlenging zou alleen expliciet doelgebonden opgenomen mogen worden.
- Specificeer duidelijker wat 'niet meer nodig zijn' betekent in de context van toezicht.

Door deze punten te adresseren in de definitieve versie van het Cyberbeveiligingsbesluit en de ministeriële regelingen, kan een meer werkbare en proportionele implementatie van NIS2 worden gerealiseerd voor de digitale sector in Nederland, zonder afbreuk te doen aan de cyberbeveiligingsdoelstellingen van de wetgeving.

Uiteraard is NLdigital beschikbaar voor toelichting op alle ingebrachte punten en om mee te denken over alternatieve uitwerkingen.