Vereniging NLconnect
Dr. Kuyperstraat 5
2514 BA Den Haag

T +31 70 3053333
E info@nlconnect.org
I www.nlconnect.org

Den Haag, 28-03–2025

Reactie NLconnect op consultatie Cyberbeveiligingsbesluit (Cbb), Ministeriële Regeling H.4 Cbb en Besluit weerbaarheid kritieke entiteiten (Bwke)

NLconnect is de brancheverenigingvan de telecom- glasvezel- en breedbandindustrie en behartigt de belangen van zo'n 90 partijen uit de keten van bedrijven die breedbandnetwerken aanleggen en exploiteren, bedrijven die elektronische communicatiediensten leveren over deze digitale infrastructuur alsmede partijen die aan deze keten toeleveren.

Als branche is het onze ambitie om de voorsprong die ons land heeft op het gebied van digitale connectiviteit te behouden en uit te bouwen door ervoor te zorgen dat elke Nederlander en elk Nederlands bedrijf de beschikking heeft over uitmuntende en veilige breedbandverbindingen. Dat vraagt ook van onze leden om voortdurende investeringen in digitale weerbaarheid.

In het Cyberbeveiligingsbesluit worden regels uit de Cyberbeveiligingswet uitgewerkt. We stellen het bijzonder op prijs in de gelegenheid te worden gesteld te reageren op deze consultatie. We maken graag de volgende opmerkingen en doen de volgende verzoeken tot verduidelijking en aanpassing:

1. Samenloop Cbw en Wwke

Ten aanzien van de mogelijke samenloop van de Cbw en Wwke (en het Cbb en Bwke) heeft NLconnect twee verzoeken en wel voor de volgende onderwerpen:

1) Onduidelijkheid toepasbaarheid van de zorg- en meldplicht van Wwke voor telecomoperators.
2) De bewoording van het Cbb en de Bwke wijkt onlogisch van elkaar af.

Ad 1) Onduidelijkheid toepasbaarheid zorg- en meldplicht Wwke
In haar reacties op de consultaties van de Cbw en de Wwke dd. 1 juli 2024 heeft NLconnect al aandacht gevraagd voor reikwijdte en mogelijke overlap van beide wetten en de onduidelijkheid die dat oproept. Hoewel deze reactie de besluiten betreft meent NLconnect er goed aan te doen hier nogmaals op te wijzen omdat de invulling van de zorg- en meldplicht in de beide besluiten hier verder niet op in gaat.

In zowel de Memorie van Toelichting (MvT) op de Cbw als die op de Wwke wordt in paragraaf 2.3 aandacht besteed aan de verhouding tussen beide wetten. De teksten komen soms letterlijk overeen.

Gezien de *all hazard* benadering van de Cbw en het feit dat in artikel 24 Wwke veel verplichtingen inclusief zorg- en meldplicht, expliciet niet van toepassing worden verklaard op de digitale infrastructuur, is het moeilijk te duiden wanneer er toch sprake zou zijn van een incident dat onder

de Wwke valt ("*andere fysieke omgevingen of fysieke aspecten die de essentiële dienstverlening raken"*[1]).

Concrete voorbeelden van incidenten of bijna-incidenten die gevolgen hebben die zowel de netwerk- en informatiesystemen als andere fysieke aspecten van de essentiële dienstverlening raken zijn op dit moment niet voorhanden.

NLconnect verzoekt daarom nogmaals de paragrafen 2.3 in de MvT's op beide wetten hierop aan te passen en te verduidelijken.

Ad 2) Bewoording Cbb en Bwke
Het Cbb en het Bwke gebruiken verschillende en deels overlappende bewoordingen voor vergelijkbare regelingen. Hierdoor is onduidelijk of inhoudelijke verschillen worden beoogd. Dit maakt het verwarrend voor bedrijven die onder beide regelingen vallen. Zie bijvoorbeeld art. 10 Cbb vs art. 3.2 Bwke, art. 10 Cbb vs art. 7 Bwke, art. 9 Cbb vs art. 9 Bwke, art. 15 Cbb vs art. 11 Bwke en art. 20 Cbb vs art.10 Bwke. Dit is in strijd met aanwijzing 3.7 uit de *Aanwijzingen voor de regelgeving*.

NLconnect verzoekt de Minister beide besluiten zo veel mogelijk te harmoniseren/ uniformeren. Voor zover dat niet mogelijk is verzoekt NLconnect de Minister in de toelichting uit te leggen waarom er afwijkingen in terminologie zijn.

2. Zorg- en meldplicht

De verplichtingen die in de uitvoeringsverordening zijn opgenomen bevatten zeer gedetailleerde instructies aan aanbieders van essentiële diensten. Voor aanbieders van elektronische communicatie- en netwerkdiensten betekent dit dat er minstens vier zorgplichten van toepassing kunnen worden:
(1) de generieke zorgplicht van de Telecommunicatiewet,
(2) de zorgplicht als beschreven in het Cbb,
(3) de zorgplicht als beschreven in het Bwke (voor zover die van toepassing zou zijn) en (4) de verplichtingen die worden opgelegd met het Besluit en de Regeling Veiligheid en Integriteit Telecommunicatie (die alleen voor mobiele netwerk operators geldt).

Daarnaast hebben aanbieders te maken met
(5) de Uitvoeringsverordening (zie hiervoor ook paragraaf 3, verderop), die feitelijk van toepassing wordt op specifieke diensten die door de NLconnect-leden worden geleverd, waardoor er potentieel nog elf specifieke zorg- en meldplichten worden toegevoegd
In de praktijk is het technisch vrijwel onmogelijk om strikt onderscheid te maken tussen netwerk- en informatiesystemen die uitsluitend voor diensten en netwerken zoals genoemd in artikel 1 van de Uitvoeringsverordening worden gebruikt en die welke ingezet worden voor de netwerken en diensten die onder het Cbb vallen.

Daarmee brengt de Uitvoeringsverordening het aantal verplichte na te leven zorg- en meldplichten op vier tot vijftien. NLconnect verwacht dat door RDI zal worden toegezien op naleving, maar met de beschreven stapeling van plichten zullen de aanbieders overbelast worden met het afleggen van verantwoordelijkheid en de RDI met het verwerken ervan. En dan hebben wij het nog niet over alle andere onder toezicht gestelde sectoren en hun toezichthouders die met gelijke stapelingen worstelen. Terwijl een enkele zorgplicht voor de telecomsector en misschien wel voor alle essentiële aanbieders voldoende zou moeten zijn.

[1] Memorie van Toelichting Wwke versie 11 december, paragraaf 2.3, ook vijfde alinea

NLconnect verzoekt de Minister om in de toelichting te verduidelijken hoe hij de stapeling van zorgplichten ziet, hoe deze leidt tot meer beoogde veiligheid en hoe deze stapeling leidt tot efficiënte regelgeving en toezicht.

3. Artikel 4 Cbb: Toepassingsbereik

In de Nota van Toelichting op het Cbb bij artikel 4 is opgenomen dat, indien een entiteit zowel van een soort als bedoeld in artikel 1 Uitvoeringsverordening als een ander soort als bedoeld in bijlage 1 en 2 van de Cbw is, zowel de zorgplicht- en meldplichtverplichtingen uit de uitvoeringsverordening als die bij of krachtens het Cbb van toepassing zijn. Een voorbeeld hiervan is een entiteit die zowel een aanbieder van cloudcomputingdiensten als een aanbieder van internetknooppunten is. Deze entiteit heeft zowel nadere zorg- en meldplichten op grond van de Uitvoeringsverordening, namelijk in haar hoedanigheid van aanbieder van cloudcomputingdiensten, als op grond van het Cbb in haar hoedanigheid van internetknooppunt.

NLconnect leest in deze toelichting dat het relevante bedrijfsonderdeel dat valt onder het Cbb moet voldoen aan de zorgplicht onder het Cbb en niet de entiteit als geheel. NLconnect verzoekt de Minister om in dezen verduidelijking op te nemen in de toelichting. Zo mogelijk moet voorkomen worden dat zorg- en meldplichten voortvloeiend uit de Uitvoeringsverordening en het Cbb door elkaar heen gaan lopen.

4. Artikel 6.3/12.1/14.1

In artikel 6.3 Cbb, 12.1 Cbb en 14.1 Cbb wordt de volgende zin gebruikt:
"(…) en andere binnen de entiteit werkzame personen". Dit is een zeer ruime omschrijving die moet worden ingekaderd, omdat dat een onevenredige belasting oplevert. Immers, het vergt motivatie waarom bijvoorbeeld een cafetariamedewerker, hoewel personeel, niet aan de gestelde eis hoeft te voldoen. Daarmee gaat deze bepaling verder dan artikel 21 NIS2 en artikel 21.3(j) Cbw en vormt het feitelijk een nationale kop. Dit is praktisch niet uitvoerbaar door bedrijven. Artikel 10 Bwke bevat deze uitbreiding bijvoorbeeld niet.

5. Artikel 16 Cbb

De tekst van artikel 16 Cbb is niet geheel duidelijk, noch in lijn met de praktijk. Het is gebruikelijk dat er beleid wordt vastgesteld voor het beheer van de netwerk- en informatiesystemen. De werking van netwerk- en informatiesystemen is een gevolg van onder andere beleid op het gebied van beheer, continuïteit en beveiliging.

NLconnect stelt daarom voor om de tekst van artikel 16 Cbb als volgt aan te passen:

1. *De essentiële entiteit of belangrijke entiteit* ***heeft vastgesteld beleid voor het beheer*** ~~***en de werking***~~ ***van de netwerk- en informatiesystemen*** *die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.*

6. Hoofdstuk 5 Cbb, artt. 20-23

De verplichtingen die in Hoofdstuk 5 Cbb zijn opgenomen ten aanzien van trainingen, de certificaten en de vereisten die aan de trainer worden opgelegd zijn veel verstrekkender dan hetgeen daarover is opgenomen in NIS2. De uitwerking van de opleidingsverplichting uit NIS2 in het Cbb lijkt inhoudelijk een Nederlandse kop op de Europese wetgeving te zijn. Naast de onwenselijkheid van een kop op de Europese verplichtingen bij de implementatie naar Nederlands recht is de kans groot dat de opleiding die binnen alle entiteiten zal moeten worden gevolgd een grote vertraging op zal lopen. De trainers

die aan alle beschreven eisen voldoen zijn in de markt niet in zulke grote getalen beschikbaar. Bovendien is het de vraag of de opleiders die aan de specifiek beschreven vereisten voldoen voor elke onder NIS2 vallende entiteit de meest aangewezen trainer is. Een meer algemene verplichting, zoals in NIS2, met doelomschrijving, leidt tot een passender opleiding met passender bijkomende kosten.

Als het daarnaast verplicht zou worden om externe trainers in te huren heeft dit ook een prijsopdrijvend effect op deze diensten, dat kan niet de bedoeling zijn, trainingen moeten laagdrempelig zijn, zeker voor het MKB.

NLconnect verzoekt de Minister de bepalingen in Hoofdstuk 5 zodanig aan te passen dat deze niet zwaarder worden ingevuld dan opgenomen in NIS2.

7. Art. 24 Cbb significante incidenten

De drempelwaarden voor de significante incidenten zullen later worden opgenomen in de ministeriële regelingen. NLconnect wil hierbij alvast meegeven dat deze drempelwaarden zo dienen te worden opgesteld dat deze zien op de echte significante incidenten. Het risico bij een te lage drempelwaarde is dat er talloze meldingen zullen moeten worden gedaan die niet daadwerkelijk significant zijn en die de aandacht en tijd wegnemen van de daadwerkelijk significante incidenten.

NLconnect verzoekt voor de telecompartijen zo veel mogelijk aan te sluiten bij de drempelwaarden die onder NIS1 zijn opgesteld.

8. MR algemeen

Zowel het Cbb (Amvb) als de Ministeriële Regeling onder het Cbb (MR) liggen ter consulatie. Het valt op dat in de MR veel dubbelingen zijn opgenomen van verplichtingen en verwijzingen die al in het Cbb staan. Dit komt de duidelijkheid niet ten goede. Een voorbeeld daarvan is artikel 3 MR.

NLconnect verzoekt de Minister daarom om de MR kritisch na te lopen op dubbelingen met het Cbb en waar mogelijk de dubbelingen te verwijderen. Op die manier worden discussies over onduidelijkheden, tweeërlei uitleg etc. vermeden.

9. MR Toelichting op artikel 4

De eerste zin van de op één na laatste alinea op bladzijde 10 van de toelichting op de MR loopt niet. Ons verzoek is om deze zin aan te passen.

10. MR Artikel 7

Het is gebruikelijk en passend binnen het wettelijk kader dat bij het vaststellen van de beveiligingseisen rekening wordt gehouden met een risicogebaseerde validatie. Immers, aanbieders van ICT diensten en/of producten werken ook met risicogebaseerde validatie. Dat sluit aan bij staande praktijk, zonder dat het risico groter wordt. In de MR is deze aansluiting achterwege gelaten waardoor er onduidelijkheid over zou kunnen ontstaan.

NLconnect verzoekt de Minister om de volgende (dikgedrukte) toevoeging te doen in artikel 7 lid 1 sub c van de MR:

“de vereisten voor het bewijs door leveranciers van ICT-diensten of ICT-producten dat deze voldoen aan de vermelde beveiligingseisen, bedoeld in artikel 10, tweede lid, van het Cyberbeveiligingsbesluit, alsmede documentatie van de resultaten van de ***risicogebaseerde*** *validering.”*

11. MR Artikel 9

Het is (nog) niet gebruikelijk dat dat het toewijzen en het gebruik van speciale toegangsrechten voor de logische en fysieke toegang tot netwerk- en informatiesystemen per gebeurtenis aan gebruikers worden toegekend. Dat zou namelijk betekenen dat er steeds apart toegang wordt verleend per upgrade, installatie of bij (analyse van) incidenten. Deze werkwijze zorgt voor een onacceptabele vertraging in de noodzakelijke speciale toegang tot systemen bij dienstverstorende incidenten. Door de speciale toegangsrechten toe te kennen aan een beperkt aantal beheerders, specifiek te monitoren op de werkzaamheden van de accounts met speciale toegangsrechten en de eisen voor de beveiliging van zo'n speciaal toegangsrechten te verzwaren (zoals langere wachtwoorden en MFA), kan het restrisico van misbruik zo veel mogelijk worden beperkt.

In de Cbw is opgenomen dat de entiteiten in het kader van de zorgplicht passende technische en organisatorische maatregelen moeten nemen. Bij de invulling van 'passende maatregelen' dient rekening te worden gehouden met de stand van de techniek. Gezien de huidige stand van de techniek kan niet in de MR worden opgenomen dat de speciale toegangsrechten *per gebeurtenis* aan gebruikers worden toegekend.

<u>Daarom verzoekt NLconnect om de onderstaande aanpassing:</u>

1. *De essentiële entiteit of belangrijke entiteit heeft vastgesteld beleid over het toewijzen en het gebruik van speciale toegangsrechten voor de logische en fysieke toegang tot netwerk- en informatiesystemen, welke op basis van de noodzaak* ***~~en per gebeurtenis~~*** *aan gebruikers worden toegekend, in overeenstemming met het beleid over de logische en fysieke toegang tot haar netwerk- en informatiesystemen, bedoeld in artikel 15, eerste lid van het Cyberbeveiligingsbesluit. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe.*

Vanzelfsprekend zijn wij graag en altijd bereid tot nadere toelichting,

met vriendelijke groet,

Mathieu Andriessen
Directeur NLconnect