Betreft: **Reactie CIO Platform Nederland i.v.m. consultatie Cyberbeveiligingswet (NIS2 implementatiewet)**

Den Haag, 28 juni 2024

Met circa 140 van de grootste Nederlandse bedrijven, kennisinstellingen en overheidsorganisaties vormt CIO Platform Nederland (CIOPN) de grootste Nederlandse community van zakelijke gebruikers van digitale technologie. CIOPN vertegenwoordigt organisaties uit vrijwel elke sector, waaronder: retail, maakindustrie, zorg, bouw, banken, onderwijs, (zorg)verzekeraars, logistiek en transport. Zij vormen de motor voor de digitalisering van de Nederlandse samenleving en economie.

CIOPN onderstreept het belang van de NIS2 Richtlijn en daarmee de Cyberweerbaarheidswet (Cbw) en het doel om essentiële en belangrijke organisaties in Nederland beter voorbereid te laten zijn op risico's en incidenten op gebied van cyber, die hun operaties kunnen bedreigen. Het is belangrijk dat organisaties, en de bestuurders daarvan, hun verantwoordelijkheid in dezen onderkennen en ernaar handelen, niet alleen in het belang van de eigen organisatie, maar ook in het belang van andere organisaties en de maatschappij die van hun organisatie afhankelijk zijn.

In dit licht willen we wel een algemene observatie delen. Het wetsvoorstel, en ook het wetsvoorstel ter implementatie van de Verordening Kritieke Entiteiten (CER), zijn vooral gericht op individuele entiteiten en hun cyberbeveiliging. Er wordt nog onvoldoende aandacht gegeven aan de risico's en te nemen acties tussen partijen in de diverse ketens, in het bijzonder wanneer die sectoroverstijgende werking hebben, zoals tussen de sectoren chemie en transport/logistiek, of wanneer de impact van een cyberincident zich verderop in de keten laat voelen en niet per se bij de eerste orde klant of leverancier. Te denken valt bijvoorbeeld aan de fysieke of *supply chain* impact buiten een havengebied als de digitale systemen van één van de goederen verwerkende partijen te maken krijgt met een incident. Wie is dan verantwoordelijk voor het informeren van de juiste instanties en bedrijven? Dit vergt o.i. nog verdere uitwerking.

Ook hecht CIOPN eraan te onderstrepen dat de Cbw slechts één voorbeeld is van de recent gereed gekomen, en ook binnenkort te verwachten, nieuwe regelgeving op gebied van digitale technologie en veiligheid. Het is van het grootste belang dat de implementatie van al deze nieuwe regels in nauwe afstemming tussen wetgevende, uitvoerende en toezichthoudende overheidsorganisaties én bedrijfsleven totstandkomt. Alleen door continu zicht te houden op de onderlinge samenhang tussen verschillende wetten, uitvoering daarvan en impact op het bedrijfsleven, valt deze noodzakelijke én complexe regelgeving efficiënt en effectief in te voeren in het sterkt digitaliserende Nederland.

Voordat wordt ingegaan op specifieke aspecten van wetsvoorstel en Memorie van Toelichting (MvT) wil CIOPN aangeven dat een belangrijk deel van de impact van de Cbw op organisaties nog niet goed is in te schatten zolang de AMvB niet bekend is. We dringen er dan ook bij het Kabinet op aan om op korte termijn meer duidelijkheid te verschaffen over/inzicht te geven in de tekst van de AMvB.

Dat gezegd hebbend, zijn er wat ons betreft nog wel enkele punten die aandacht behoeven in de geconsulteerde versie van de Cbw, namelijk:

1. Hoofdstuk 4 betreft de identificatie van essentiële en belangrijke entiteiten. Veel (grotere) organisaties bestaan uit meerdere of zelfs vele rechtspersonen, soms in meerdere Lidstaten van de EU of ook daarbuiten. Sommige van dergelijke rechtspersonen kunnen een activiteit uitoefenen die ze tot essentiële of belangrijke entiteit kwalificeert, terwijl andere activiteiten in het kader van de Cbw minder of niet relevant zijn. Nog onduidelijk is of een entiteit waarvan onderdelen (rechtspersonen) als essentiële of belangrijke entiteit moet worden gezien in het kader van de Cbw in het geheel op het hoogste niveau (essentieel) moet worden geregistreerd (of wordt aangewezen), of per onderdeel (rechtspersoon), en of dat dan alleen moet in de Lidstaat van de 'moederorganisatie' of in de Lidstaat van de 'dochter' of beide. Ook is onvoldoende duidelijk wie namens de organisatie(s) kan optreden in het kader van de Cbw, is dat alleen de formele vertegenwoordiger, of (ook) de verantwoordelijke voor IT of cyberbeveiliging? Dit kan in complexe organisaties nogal een uitdaging worden en veel administratieve kosten en risico's rond wettelijke vertegenwoordiging tot gevolg hebben, ook zal het doen van een melding meer tijd kosten naarmate het doen van een melding meer stappen binnen de organisatie vergt.

2. In artikel 24 wordt aangegeven dat artikel 23 niet van toepassing is op essentiële of belangrijke entiteiten als die reeds op grond van sectorspecifieke regulering risicobeheersingsmaatregelen hebben genomen die 'ten minste gelijkwaardig zijn aan de verplichtingen bedoeld in artikel 23', of een vergelijkbare uitwerking hebben (art. 24, lid 2). Onze vragen hierover zijn:

    a. Wie bepaalt dit 'ten minste gelijkwaardig zijn'?
    b. Wordt dit 'ten minste gelijkwaardig zijn' alleen geacht te zijn bepaald indien dit in richtsnoeren of AMvB is vastgelegd (art. 24, lid 3), of kan een essentiële of belangrijke entiteit dit ook onder eigen verantwoordelijkheid bepalen, of in overleg met bevoegde autoriteit laten vastleggen, voor de eigen situatie?

3. Artikel 26 regelt de governance en de verantwoordelijkheden van het 'bestuur' van belangrijke en essentiële entiteiten. Nu is voor ministeries, provincies, gemeentes en waterschappen in lid 8 verduidelijkt wie voor deze entiteiten onderdeel zijn van het bestuur. Voor private entiteiten is dit echter niet duidelijk. Om de verantwoordelijkheid goed te beleggen, is het nodig om in de wet of per AMvB te verduidelijken welke managementlaag eindverantwoordelijk is voor goede cyberveiligheidsmaatregelen en voor goede opleiding en awareness binnen de entiteit.

4. In artikel 26, lid 8 en paragraaf 5.4 MvT wordt in relatie tot overheidsinstanties aangegeven dat governance verplichtingen berusten op de ambtelijke leiding en niet de politieke leiding. Dit geeft een *buitengewoon onwenselijk* signaal en kan aanleiding vormen voor verkeerde prioriteitsvorming bij overheidsinstanties. Juist omdat dat bij schaarste aan middelen (vrijwel altijd) de politiek verantwoordelijke een belangrijke/doorslaggevende stem zal hebben in het toekennen van middelen, is het van belang dat alle betrokkenen bij die besluitvorming goed zijn geëquipeerd om het belang van cyberbeveiliging te kunnen beoordelen. Daarnaast is voorbeeldgedrag vanuit de top van elke organisatie, inclusief politieke leiding, noodzakelijk voor het opbouwen en onderhouden van een cultuur van (cyber)veiligheid.

5. Hoofdstuk 9 betreft de meldplicht. In het licht van hetgeen eerder gevraagd is rondom identificatie van essentiële en belangrijke entiteiten in geval van complexe organisaties, is de vervolgvraag in verband met de meldplicht, welke entiteit moet melden. Is dat alleen de moederorganisatie? Of alleen de dochter waar het incident plaatsvindt? Of beide? Maakt het in dit geval nog uit of de beide rechtspersonen gebruikmaken van dezelfde IT-omgeving, of niet?

6. In artikel 39 staat dat het CSIRT of de bevoegde autoriteit 'na raadpleging van de betrokken entiteit' het publiek kan informeren over een significant incident. Wat is de aard van deze raadpleging? Is het informerend ("we gaan dan en dan het publiek informeren") of heeft de entiteit nog ruimte om een eigen belang aan te geven of aanpassingen voor te stellen? Indien de entiteit een andere inschatting heeft van het belang om het publiek te informeren over het significante incident ten opzichte van belangen om dat niet te doen (bijvoorbeeld omdat er nog geen adequate oplossing is om schade bij anderen te voorkomen, of om andere redenen), staat dan bezwaar of beroep open tegen het voornemen of besluit van de bevoegde autoriteit? Op deze punten is verduidelijking nodig.

7. Artikel 42, lid 2 geeft aan dat in het geval van vrijwillige meldingen over incidenten, bijna-incidenten of cyberdreigingen, die door een essentiële entiteit gedaan zijn bij een CSIRT, de CSIRT de melding doorgeeft aan de betrokken bevoegde autoriteit indien de meldende entiteit ook kritieke entiteit is onder de Wet weerbaarheid kritieke entiteiten. Daarmee implementeert Artikel 42, lid 2 het artikel 23 lid 10 van de NIS2. In onze optiek is dit een potentieel gevaarlijke bepaling voor vrijwillige meldingen, die bovendien verder gaat dan nodig om invulling te geven aan artikel 23 lid 10 van de NIS2. Het voorgestelde artikel 42 lid 2 betekent namelijk dat dergelijke entiteiten mogelijk de juridische/risicomijdende afweging gaan maken om de vrijwillige melding helemaal niet te doen. Dat hoeven ze immers niet en houdt wel een risico van nader onderzoek en eventuele maatregelen door de bevoegde autoriteit in.

   Een dergelijke afweging van de entiteit betekent dat minder informatie voorhanden is bij de CSIRT, die daardoor minder '*situational awareness*'

kan opbouwen, waardoor mogelijke kwetsbaarheden en incidenten later worden onderkend en hierop later kan worden gehandeld.

In onze optiek is het van het grootste belang dat bij de CSIRT zoveel mogelijk relevante meldingen binnenkomen over incidenten, bijna-incidenten, kwetsbaarheden en andere relevante indicatoren, om zo goed mogelijk zicht te hebben op de cybersecurity gerelateerde ontwikkelingen in het land. Alle drempels die dergelijke informatiedeling in de weg staan, dienen te worden vermeden of gemitigeerd. Derhalve zouden vrijwillige meldingen niet zomaar moeten worden gedeeld met de bevoegde autoriteit, in ieder geval niet onverwerkt of zonder inspraak van de vrijwillig meldende essentiële entiteit. Tot algemene inzichten verwerkte adviezen en waarschuwingen dienen vanzelfsprekend wél te worden gedeeld, maar zonder directe verwijzing naar de kritieke entiteit(en) die informatie hebben aangeleverd. Indien direct wordt verwezen naar de kritieke entiteit, moet dit bij vrijwillige meldingen met inspraak zijn van de entiteit zelf. Op die wijze kan nog steeds invulling worden gegeven aan de eis voor CSIRT's en bevoegde autoriteiten om informatie te verschaffen over (vrijwillig) gemelde incidenten door kritieke entiteit aan de autoriteiten onder de Verordening Kritieke Entiteiten (CER).

8. Artikel 56 betreft het samenwerken en uitwisselen van informatie tussen bevoegde autoriteiten met het oog op een doeltreffende en doelmatige uitvoering van hun taken. In de MvT wordt in paragraaf 5.7.13 e.e.a. nader toegelicht waarbij wordt aangegeven dat deze samenwerking o.a. ziet op voorkomen van onevenredige toezichtslasten en consistente uitleg van begrippen en normen uit de wet.

   CIOPN juicht dit toe, omdat deze wet niet uitsluit dat een organisatie met meerdere bevoegde autoriteiten te maken krijgt, wat het risico in zich draagt dat die autoriteiten eigen interpretaties hanteren, andere normen hanteren, rapportage formats of verschillende maatregelen ter afdekking van hetzelfde risico vereisen en ongecoördineerd bezoeken afleggen. Dit alles drijft de lasten voor de onder toezicht staande entiteit enorm op, terwijl de cyberbeveiliging daarmee niet of nauwelijks wordt verbeterd. Dit moet worden voorkomen.

   In de MvT is sprake van een samenwerkingsprotocol, dit komt wat vrijblijvend over. Hoe verzekert de wetgever dat dergelijke samenwerking daadwerkelijk op geharmoniseerde en (ook) voor de onder toezicht staande entiteiten op efficiënte wijze tot uitvoering wordt gebracht? Bij wie kan een entiteit terecht indien in de praktijk de samenwerking tussen de bevoegde autoriteiten te wensen overlaat en tot onevenredige toezichtslasten leidt?

9. Artikel 71 betreft openbaarmaking van overtredingen. Daarin is de essentiële entiteit die een overtreding heeft begaan degene die de openbaarmaking verricht, eventueel onder verplichting van de bevoegde

autoriteit. Wat is de reden om tot deze vorm van openbaarmaking te komen? Kan de autoriteit ook zelf tot openbaarmaking overgaan, zoals in artikel 39?

10. Dezelfde vragen gaan ook op voor artikel 81, met betrekking tot openbaarmaking van overtredingen door belangrijke entiteiten.

11. Artikel 80 betreft een gerichte beveiligingsaudit bij een belangrijke entiteit. Bij belangrijke entiteiten vindt toezicht ex post plaats, dus na bijvoorbeeld een melding of een incident. Het ligt voor de hand dat de audit zich in dat geval ook dient te beperken tot de situatie die in de melding wordt genoemd, omdat anders de belangrijke autoriteit alsnog voor onevenredige maatregelen en lasten kan komen te staan. Een dergelijke beperking staat echter, wat ons betreft en onrechte, niet in het wetsartikel. Wij dringen aan op aanvulling van artikel 80 met deze beperking.

12. In paragraaf 5.3.4 van de MvT wordt e.e.a. gezegd over de beveiliging van de toeleveringsketen. Het gaat dan volgens de MvT om de relatie van entiteiten en hun rechtstreeks leveranciers of dienstverleners. Dit vergt wat ons betreft wat meer duiding. Zo komt het vaak voor dat entiteiten hun software(pakketten) afnemen via een tussenpartij, die de commerciële en operationele relatie heeft, maar geen of zeer beperkt invloed heeft op de software zelf of de pakketsamenstelling. Hoe dient een entiteit dan de beveiliging gerelateerde aspecten te regelen, wanneer die verder gaan dan instellingen (die veelal door de entiteit zelf of door de implementatiepartner kunnen worden ingesteld) en bijvoorbeeld de softwarecode of samenstelling van softwarepakketten betreffen. Ook op gebied van Clouddiensten is vaak een hele keten van partijen betrokken.

    Beperkt de verantwoordelijkheid/zorgplicht van de entiteit zich alleen tot de partij waarmee ze zelf een overeenkomst aangaat, of verder? Hoe wordt voorkomen dat leveranciers van de kernfunctionaliteit waaraan de entiteit behoefte heeft en die veilig moet blijven, zich onttrekt aan eigen verantwoordelijkheid door een schil van tussenpartijen te gebruiken die de relatie met de entiteit onderhouden? Er is grote behoefte aan meer duiding van de zorgplicht op dit punt. Hier kan invulling aan worden gegeven middels een leidraad van de toezichthouders.

13. In paragraaf 5.3.5 MvT wordt in de tweede alinea aangegeven dat in de AMvB naar verwachting gebruik wordt gemaakt van de ruimte die de NIS2 Richtlijn biedt om nationaal maatregelen te stellen die een hoger beveiligingsniveau waarborgen dan uit de richtlijn zelf volgen. Dit verhoudt zich slecht tot het uitgangspunt uit het Hoofdlijnenakkoord dat er geen nieuwe nationale koppen komen op Europees beleid (paragraaf 10.1). De oproep is om doelmatig om te gaan met aanvullende nationale regels, bovenop dat wat wordt vereist in de NIS2 Richtlijn.

14. In paragraaf 5.6.4 MvT wordt aangegeven dat partijen die informatie krijgen van de CSIRT de benodigde maatregelen moeten treffen om die

informatie te beveiligen, en eventuele persoonsgegevens moet verwerken conform de AVG. Nu is de door Autoriteit Persoonsgegevens gehanteerde definitie van persoonsgegevens wat ruimer dan wat in het gangbare taalgebruik onder persoonsgegevens wordt verstaan, denk aan IP-adressen. Voor partijen die persoonsgegevens ontvangen van de CSIRT, moet duidelijk zijn dat dit het geval is, en of hier al dan niet een verwerkingsovereenkomst voor nodig is voordat de informatie kan worden verwerkt.

15. In paragraaf 8.1.3 MvT wordt aan het eind van de 2e alinea aangegeven dat een schatting is gemaakt dat zo'n 1.000 meldingen per jaar worden gemaakt. We gaan er van uit dat dit gaat om het aantal meldingen dat bij de NCSC binnen zal komen. Mocht dit gaan om het aantal meldingen dat per entiteit wordt verwacht, behoeft dit nog enige verduidelijking. Het verdient aanbeveling dat in dezelfde alinea genoemde parameters gestuurd gaat worden op het beperken van het aantal meldingen dat per entiteit nodig is tot het hoogstnoodzakelijke.

We zijn beschikbaar om nadere toelichting te geven op het voorgaande en blijven ons inzetten om, o.a. via de PPS NIS2 implementatie, te helpen de implementatie van NIS2 en de Cbw in Nederland zo efficiënt en soepel mogelijk te laten verlopen.

Namens CIO Platform Nederland,

Ronald Verbeek

Directeur