Reactie CIO Platform Nederland i.v.m. consultatie Cyberbeveiligingswet (NIS2 implementatie)

Met zo'n 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, de Cyberweerbaarheidswet (Cbw) en het doel om essentiële en belangrijke organisaties in Nederland beter voorbereid te doen 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.

Het is goed dat nu ook het concept van het Cyberbeveiligingsbesluit (Cbb) en de ministeriële regeling (MR) bekend zijn gemaakt en ter consultatie zijn aangeboden. Hierin staan nadere uitwerkingen van de verantwoordelijkheden en verplichtingen voor de essentiële en belangrijke entiteiten die onder de Cbw vallen. Het valt op dat hier wel erg wordt ingestoken op het hebben van beleid en 'papierenveiligheid' en weinig concreet wordt over het veilig zijn in de praktijk.

Voor de efficiënte en effectieve implementatie en werking van deze wet is ook van groot belang dat het toezicht door de toezichthouders geen onnodig grote belasting oplevert voor essentiële en belangrijke entiteiten. Daarvoor is coördinatie en harmonisering van o.a. rapportageverplichtingen tussen de toezichthouders noodzakelijk, liefst internationaal (voor internationaal opererende entiteiten). Hiervoor vraagt CIOPN extra aandacht.

In het kader van de consultatie van het Cbb zijn er wat ons betreft nog wel enkele punten die aandacht behoeven in de huidige versie, namelijk:

1. Het is te zien dat in het Cbb de balans wordt gezocht tussen enerzijds de vrijheid laten aan de organisatie die onder de Cbw valt om maatregelen te treffen in overeenstemming met de risicoanalyse die het heeft gemaakt en anderzijds aan te geven wat in ieder geval aan beleid of maatregelen wordt verwacht. Het is o.i. wenselijk om vroeg in het besluit of de nota van toelichting aan te geven en daarbij te benadrukken dat de verantwoordelijkheid uiteindelijk ligt bij de bestuurder van de essentiële of belangrijke entiteit, die handelt op basis van de uitkomsten van de risicoanalyse.

2. In diverse artikelen in het Cbb worden minimale vereisten neergelegd (aangegeven door o.a.: '…in ieder geval…' , '… bevat ten minste …'). Het is wenselijk in de nota van toelichting te verduidelijken of dergelijk beleid/dergelijke maatregelen samen in een beleidsdocument mogen worden opgenomen. Dat zou wenselijk zijn, omdat het de integraliteit van maatregelen bevordert.

3. Het Cbb wijst op een aantal plaatsen nogal breed naar netwerk- en informatiesystemen, bv. in art. 10, lid 1. Gaat het hier echt om álle netwerk- en informatiesystemen, of alleen die netwerk- en informatiesystemen die van belang zijn voor het onderdeel/de onderdelen van de entiteit die kritisch zijn voor het proces/product/de dienst waardoor de entiteit onder de NIS2/Cbw valt. Het is bijvoorbeeld voorstelbaar dat er bij een entiteit een systeem is waarin kantoorartikelenvoorraden, of keukenvoorraden wordt bijgehouden en bestellingen worden gedaan bij de leverancier en dat helemaal los staat van de onder NIS2-vallende activiteit. Moeten daarvan ook de afhankelijkheden worden vastgelegd, of alleen indien/voor zover ze de kritische activiteit?

4. Artikel 11 Cbb geeft enige vrijheid aan de entiteit door te stellen dat 'waar mogelijk' eisen over beveiliging deel moeten uitmaken van overeenkomsten met leveranciers. Hoewel dit enerzijds tegemoet komt aan de praktijk van ongelijke onderhandelingsposities en moeite om eisen te stellen aan grote leveranciers (bv. Big Tech, maar ook grote OT-leveranciers), en ook de verzekering geeft aan leveranciers om niet aan elke min of meer willekeurig gestelde eis van uiteenlopende klanten te moeten voldoen, levert dit ook aan de leverancier de vrijheid op om zijn/haar eigen speelruimte te maximaliseren en zich überhaupt niet te conformeren aan ook redelijke een breed gestelde eisen. Kan hier een formulering worden gevonden die de druk op leveranciers om aan (gestandaardiseerde) eisen te voldoen maximaliseert, terwijl het de entiteiten niet wordt aangerekend als ze kunnen aantonen dat het door onwil van de leverancier is dat niet aan de gestelde eisen wordt voldaan en niet eenvoudig een alternatief voorhanden is. Of wordt dit op termijn al voldoende geregeld in de Cyber Resilence Act?

5. Artikel 11 Cbb richt zich kennelijk uitsluitend op software, hardware en diensten die ze afnemen van leveranciers en waaraan eisen moeten worden gesteld. In het Cbb staat nergens dat de software, hardware en diensten die essentiële of belangrijke entiteiten zelf ontwikkelen voor eigen gebruik ook moeten voldoen aan die eisen. Of is dat de bedoeling van lid 2 van dit artikel? Dan zou dan wat explicieter moeten worden vermeld.

6. Artikel 14, lid 3, Cbb geeft aan dat betrouwbaarheidseisen moeten worden gesteld aan beveiligingsmedewerkers. Er staat echter niets over bekwaamheid van dat personeel, is dat niet (ook) wenselijk? Of is dat afdoende geregeld in artikel 12, lid 2? Verduidelijking is hier wenselijk.

7. Artikel 16, lid 3 Cbb stelt dat een entiteit een 'volledige en actuele inventaris van informatie en andere gerelateerde netwerk- en

informatiesystemen' heeft en bijhoudt. Dit is erg generiek gesteld. Betreft het om categorieën informatie, of over elk data-element? Betreft het alleen de informatie en systemen die van belang zijn voor de kritische activiteiten van de entiteit, of alles binnen de entiteit?

8. Artikel 20 Cbb betreft training van het bestuur van de entiteit. Het lijkt te gaan over leden van de Raad van Bestuur en niet leden van de Raad van Commissarissen/Toezicht. Klopt dat? Dat lijkt niet wenselijk, want ook in die gremia moet het juiste gesprek worden gevoerd.
   Wat ook niet helemaal duidelijk wordt is in hoeverre en gaat om de 'persoon' die de training krijgt, of de 'persoon in de context van de entiteit'? Het komt nl. vaak voor dat personen die in één entiteit lid zijn van de RvB, in andere entiteit(en) een rol heeft in de RvC/RvT. Is die persoon dan klaar als hij/zij in het kader van de RvB-rol een training heeft gehad, of moet die ook een training volgen in het kader van elk van de RvC/RvT-rollen? En hoe zit dat als een persoon RvB-rollen vervult voor diverse entiteiten die onder één holding/groep van ondernemingen?

9. Door de eisen aan de training, trainer en certificaat (artikelen 21-23 Cbb), lijkt de wetgever verder te gaan dan in de NIS2 richtlijn is aangegeven en ook verder dan andere lidstaten van de EU in hun implementatie lijken te gaan. Wordt hier niet toch een 'nationale kop' op Europees beleid gezet? En hoe verhoudt dat zich tot het uitgangspunt in de Hoofdlijnenakkoord van de regerende coalitie dat dit niet zou worden gedaan?

10. Artikel 22 Cbb (eisen aan de trainer). Hier wordt verwezen naar artikel 24, vijfde lid van de wet. Die wet kent echter geen vijfde lid van artikel 24. Waarschijnlijk wordt bedoeld artikel 26, vijfde lid.

11. Artikel 22 Cbb (eisen aan de trainer). Hier wordt ingezet op een onafhankelijk trainer. De Cbw stelt in artikel 26, vijfde lid, dat een lid van bestuur aantoonbare kennis heeft en dat moet aantonen door een certificaat van deelname aan een training die onderwerpen uit lid 2 van dat artikel behandelt. Onduidelijk gemotiveerd is, waarom in het Cbw dit zodanig wordt ingevuld dat de training alleen door een onafhankelijke trainer mag worden gegeven; het zorgen voor een goedgevulde orderportefeuille van aanbieders van trainingen is toch geen doelstelling van deze wet? En het onnodig op kosten jagen van onder Cbw vallende entiteiten zou dat ook niet moeten zijn.
    Afhankelijk van de aard en omvang van de entiteit en de hierbij te trainen groep aan mensen, zou het o.i. mogelijk moeten zijn een interne medewerker, met aantoonbare en minimaal gelijkwaardige ervaring als die aan de onafhankelijke trainer wordt gesteld, te mogen inzetten in plaats van een onafhankelijke trainer. In lijn hiermee zouden de eisen aan het certificaat aangepast moeten worden.

12. Hoofdstuk 6 (Meldingen). Hoe dienen essentiële en belangrijke entiteiten om te gaan met incidenten bij leveranciers waarbij er wel het vermoeden bestaat dat de eigen onderneming daarvan een risico ondervindt, maar er onvoldoende gegevens beschikbaar worden gesteld door de leverancier om dit expliciet te kunnen duiden?

13. Artikel 31 Cbb lijkt een dubbel meldplicht op te leggen aan financiële entiteiten. In hoeverre gaat dit een dubbele administratieve last opleveren voor die entiteiten, of wordt de melding door het eerste meldpunt gedeeld met andere instanties en is de last dus beperkt. Dit zou de voorkeur hebben en lijkt ook in eerdere instantie te zijn gecommuniceerd.

14. Cbb Nota van Toelichting p.3 (Structurele regeldruk). In deze paragraaf is aangegeven dat 'Bedrijven verwachten met name kosten te maken bij de beoordeling van risico's in de toeleveringsketen, omdat verder gekeken moet worden in de keten dan alleen de directe leveranciers.' Dat lijkt terecht, omdat de directe leverancier niet altijd degene is die controle heeft op het onderdeel (software/hardware) dat een risico oplevert voor de continuïteit van kritische operaties. Software wordt bv. vaak geleverd tussenpartijen die per beperkt in kunnen grijpen in de software zelf als daar zich een incident manifesteert. Is de focus op eerste orde leveranciers in deze niet teveel window-dressing en verhult dat niet teveel de daadwerkelijke impact?

Ook bij de ministeriële regeling hebben we nog enkele vragen:

1. Artikel 3, lid 2 onder a MR: betreft dit doelstellingen voor de beveiliging van alle systemen, of alleen de systemen die direct nodig zijn voor het leveren van de producten/diensten waardoor de entiteit onder NIS2/Cbw valt?

2. Artikel 6 onder a MR: zoals ook bij het Cbb al gesteld is dit soms ingewikkeld of niet mogelijk, vanwege de afhankelijkheid van informatiedeling door leveranciers verderop in de keten. Leveranciers hebben eigen belangen om selectief informatie te delen. En tussenpartijen hebben zelf mogelijk ook niet de informatie of mogelijkheid om incident te verhelpen.

3. Artikel 7, lid 1 MR: zoals ook bij het Cbb al gesteld is de vraag of dit ook expliciet geldt voor zelf ontwikkelde producten/diensten. Kan dat duidelijker worden aangegeven.

4. Artikel 7, lid 3 MR: Vreemde verwijzing. Artikel 21 Cbw heeft geen leden en artikel 21 Cbb geen derde lid.

5. Toelichting op artikel 4, p.10 bovenste paragraaf. Zou er niet iets behoren te staan over prioritering van aanpak van risico's, of valt dat volledig binnen de eigen afweging van de entiteit?

Nog enkele moeilijk lopende zinnen in de ministeriële regeling:

- Toelichting op artikel 4, p.10, een na laatste paragraaf 'Onderdeel d …'. Deze zin loopt niet.
- Toelichting op artikel 6, p.12, laatste paragraaf 'Hiermee wordt de kans verkleind dat… de cascade effecten van zo'n incident worden beperkt.'. Die effecten zouden juist wel moeten worden beperkt. De zin loopt klaarblijkelijk niet goed.
- P.14, tweede alinea, zin 'Indien … , kunnen essentiële en belangrijke entiteiten een plan op te stellen en uit te voeren om …'. Zin loopt niet.

CIO Platform Nederland is beschikbaar om nadere toelichting te geven op het voorgaande en blijft zich inzetten om te helpen de implementatie van NIS2, de Cbw en onderliggende regelgeving in Nederland zo efficiënt en soepel mogelijk te laten verlopen.