Bevindingen CBW door Omni-U Services B.V.

Bijlage 1 en 2 CBW vs Bijlage I en II NIS2

Bijlage I en II van de NIS2 zijn niet als optioneel beschreven in de NIS2. Toch staan er in deze draft een aantal aanpassingen. Consequentie is dat hierdoor het toepassingsgebied van de Cyberbeveiligingswet anders wordt dan de intentie van de NIS2 - sommige entiteiten worden nu potentieel uitgesloten die wel in de scope hadden moeten staan, anderen worden toegevoegd terwijl ze eigenlijk niet in de scope staan. Hieronder de afwijkingen:

- Bijlage 1:
    - Zorgaanbieder onder de WKKGZ is anders gedefinieerd dan in Richtlijn 2011/24/EU. Die laatste is naar mijn idee iets duidelijker. WKKGZ blijft steken op de definitie van het woord "zorg" door te koppelen aan WLZ, ZVW en "andere zorg".
    - "gemeenten, alsmede gemeenschappelijke regelingen voor zover deze laatste kwalificeren als entiteit van het in bijlage I of II van de NIS2-richtlijn" is toegevoegd aan de originele Bijlage I waardoor wij nu Gemeenten als essentieel bestempelen terwijl dit in de NIS2 richtlijn niet aan de orde lijkt te zijn.
- Bijlage 2:
    - Er is een specificatie toegevoegd aan de soort entiteit Onderzoeksorganisaties. Deze specificatie bestaat niet in Bijlage II van de NIS2 richtlijn. Sluiten wij hiermee dus organisaties uit die potentieel wel bedoeld zijn onder de NIS2 richtlijn?

Artikel 1 CBW:

- Waarom is de definitie van "aanbieders van internetknooppunten" uit de lijst gehaald en vervolgens bij het soort entiteit in Bijlage 1 er aan toegevoegd. Dit is niet consistent. Mijn voorstel is om dit terug te brengen in lijn met de NIS2.

Artikel 4 CBW:

- Artikel 4, lid 2, lid 3: Door ze uit te zonderen van lid 1 is nu te lezen dat de entiteiten die op basis van deze leden niet als essentieel of belangrijk geclassificeerd worden. Dat is niet conform de intentie NIS2 (o.a. overweging 15).
- Artikel 4, lid 3: punt c en e t/m k lijken af te wijken van de NIS2 richtlijn en daardoor wellicht disproportioneel. Door ze hier te plaatsen valt iedere onderneming van micro tot groot onder het toepassingsgebied.
- Artikel 4, lid 3 in combinatie met lid 5: Dit zijn potentieel duizenden entiteiten, inclusief micro en kleine entiteiten die niet in Nederland gevestigd zijn. Is het realistisch om zulke bedrijven deze eisen te stellen? Hier zou ik toch kijken naar grote ondernemingen in plaats van allemaal om het realistisch en hanteerbaar te houden.

Artikel 4a CBW:

- Dit wijkt af van richtlijn 2022/2557 in combinatie met artikel 2, lid 3 van de NIS2 waarin de entiteiten die onder het toepassingsgebied verklaard worden ook onder NIS2 vallen. Dit artikel laat niet alleen de geselecteerde entiteiten, maar alle entiteiten van dat soort onder de NIS2 vallen. Daardoor komen dus ook alle niet-kritieke (vaak micro en kleine) entiteiten ook binnen het toepassingsgebied van deze wet.
- De term “type entiteit” komt niet overeen met de term die in bijlage 1 gebruikt wordt (“soort entiteit”).

Artikel 5 CBW:

- Memorie van toelichting zegt het volgende: "Wellicht ten overvloede wordt opgemerkt dat de drie bijzondere gemeenten van Nederland Bonaire, Sint Eustatius en Saba buiten het bereik van de Richtlijn vallen, omdat de Richtlijn enkel van toepassing is op Europees Nederland." Echter, artikel 5 verklaard de hele Nederlandse exclusieve economische zone onder de NIS2. Daarmee zou het Caribisch gebied daar dus ook onder vallen.

Artikel 8 CBW:

- Artikel 8, lid 1h: Dit lijkt in strijd met de bepaling in de NIS2 waarin alleen centrale overheid en grote regionale overheid als essentieel bestempeld worden (NIS2 artikel 3, lid 1a en 1d). Andere overheidsentiteiten zouden daarmee als belangrijk geclassificeerd worden (NIS2 artikel 3, lid 2).
- Artikel 8, lid 1h: Gemeenten worden als essentieel geclassificeerd. Op basis van welk criterium in de NIS2 is dit gebaseerd? Ik kan geen indicatie vinden in NIS2 artikel 3, lid 1 dat de gemeenten als type essentieel geregistreerd zouden moeten staan.

Artikel 9 CBW:

- Artikel 9, lid 1b: Voor Veiligheidsregio's is dit in combinatie met artikel 6, lid 1 zeer onduidelijk. In beide gevallen wordt gesproken van openbare veiligheid.

  Een eerdere verklaring op de site van de digitale overheid (https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/) en zo ook de Memorie van toelichting geven aan dat de Veiligheidsregio buiten de scope is. Zij vallen echter wel onder de BIO die op zijn beurt de NIS2 vereisten integreert. Daarnaast gaan de gemeenten toch eisen opleggen aan hun partnerketen. Is het dus niet beter om de VRs wel onder de scope te laten vallen en gebruik door gebruik te maken van NIS2, artikel 2 lid 6 waarbij bepaalde informatiedeling die staatsgevoelig is niet gedeeld hoeft te worden?

Artikel 17 CBW:

- Artikel 17, lid 6a: waarom worden entiteiten die domeinnaamregistratiediensten verlenen hier apart genoemd? Dit is overigens ook een probleem in de NIS2 zelf. Overweging 15 van de NIS2 stelt dat "Entiteiten die voor de naleving van de maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportageverplichtingen binnen het toepassingsgebied van deze richtlijn vallen, moeten worden ingedeeld in twee categorieën, essentiële entiteiten en belangrijke entiteiten..." Domeinnaamregistratiediensten zouden daarmee dus ook ingedeeld moeten worden als essentieel of belangrijk. Het gebrek aan classificatie van de domeinnaamregistratiediensten levert veel inconsistenties op (o.a. artikel 17, lid 2 en lid 3, artikel 23, artikel 26, artikel 28, etc). De memorie van toelichting gaat erop diep op in en ziet dit als een losstaande classificatie. Ik zie de meerwaarde niet om deze groep apart te behandelen en eigenlijk uit te sluiten van alle maatregelen. Ik vermoed dan ook dat deze groep gewoon onder essentieel of belangrijk moet vallen. Het lijkt meer onoplettendheid in de NIS2 dan een bewuste keuze.

Artikel 23 CBW:

- Artikel 23, lid 4: terminologie (Type entiteit) is inconsistent met de terminologie van de Bijlagen (Soort entiteit).
- Artikel 23, lid 4: Het ontbreken van de amvb mbt de maatregelen zoals vastgesteld in artikel 21 lid 2 van de NIS2 zorgt voor een onvolledig beeld van het effect van deze wetgeving. Wanneer kunnen we deze verwachten en gaan er per sector eigen amvb komen?

Artikel 26 CBW:

- Artikel 26 lid 2 t/m 7: De term bestuur is onvolledig (en in enkele gevallen wellicht disproportioneel). Ik zou hier de term leidinggevenden prefereren (een wat juistere vertaling van wat de Engelse NIS2 "members of management bodies" noemt). De memorie van toelichting komt eigenlijk tot dezelfde conclusie (hoofdstuk 5.4), maar geeft ook hier geen concrete definitie. Mijn voorstel is om in artikel 1 van de CBW een definitie van bestuur op te nemen (of van leidinggevenden), waaruit duidelijk wordt over welke management laag/lagen het gaat.
- Artikel 26, lid 7: We zetten hier een stuk hoofdelijke aansprakelijkheid van de bestuurders op. Maar hoe rijmt dit met het BW? Een bestuurder kan persoonlijk aansprakelijk gesteld worden voor wanbeleid of wanbestuur onder bepaalde omstandigheden, zoals beschreven in Burgerlijk wetboek 2, artikel 9. Deze introductie lijkt een eerste stap in het omverwerpen van het concept waarop de BV zijn bestaansrecht heeft.
  Ik constateer overigens dat in § 16.2 deze aansprakelijkheid niet genoemd wordt. Heeft dat met deze haalbaarheid te maken? Ik zou in ieder geval een onderbouwde keuze maken: ofwel consistent volgen en opnemen, ofwel helemaal achterwege laten.

Artikel 48 CBW:

- Artikel 48, lid 1d: Entiteit die domeinnaamregistratiediensten verleent staat niet in bijlage 1 van de CBW. Dat zou een hoop onduidelijkheid schelen.

Artikel 50 CBW:

- Artikel 50, lid 3: Er staan de nodige punctuatie, spelling en grammatica fouten door de hele wet. Die laat ik aan jullie over. In dit lid staat echter het woord "maem". Ik gok dat dat het woord "maken" had moeten zijn.

§ 16.2

- Ik mis in de artikelen het recht op inspectie zoals beschreven in artikel 32 lid 2a van de NIS2. Artikel 70a lijkt hier het dichtste bij te komen met een ad hoc audit, maar daar ligt de verantwoordelijkheid voor initiatie bij de entiteit. Bij een inspectie ligt dat initiatief bij de competente autoriteit.
- Hoofdelijke aansprakelijkheid voor wettelijke vertegenwoordigers zoals beschreven in artikel 32 lid 6 van de NIS2 lijkt niet overgenomen te zijn in de artikelen van de CBW. Gezien de houdbaarheid t.o.v. BW kan ik me er iets van voorstellen, maar dit is wel een verplichte clausule.

§ 16.4

- Gezien de insteek van overweging 15 uit de NIS2, zijn de artikelen 85 t/m 88 overbodig, evenals alle andere specifieke referenties aan domeinnaamregistratiediensten.