Reactie NLdigital op Cyberbeveiligingswet, de Nederlandse implementatie van de NIS2-richtlijn

Juli 2024

Reactie NLdigital op de Cyberbeveiligingswet, de Nederlandse implementatie van de NIS2-richtlijn.

NLdigital staat positief tegenover de doelen van de vernieuwde Network & Information Systems richtlijn (NIS2). Het verhogen van de cybersecurity van iedereen streeft NLdigital met onze leden na en zien we ook als een van de grote prioriteiten van deze tijd. Wij onderstrepen de inzet dat cybersecurity niet meer slechts als een optie wordt gezien, maar dat het een voorwaarde is voor het leveren van diensten. Voor de effectiviteit daarvan is het essentieel dat dit internationaal wordt aangevlogen en niet in ieder land op zichzelf.

De Nederlandse implementatie van de wet, de Cyberbeveiligingswet (Cbw), roept echter vooralsnog meer vragen bij ons op dan dat deze beantwoordt. In deze reactie gaan we eerst in op de volgende hoofdpunten, in bijlage 2 staan specifieke opmerkingen per artikel uitgewerkt.

1. De Cyberbeveiligingswet biedt weinig duidelijkheid en verzwakt ondernemerszekerheid in haar huidige vorm; de implementatie is nog verre van volledig.

2. Het web van meerdere toezichthouders, verschillende CSIRTs en overlapping met andere wetten leidt in potentie tot onduidelijke vereisten en een stapeling van meldplichten. Hoe gaat dit voorkomen worden?

3. Er is sprake van vergaand toezicht welke zonder doelbinding inzetbaar is. Is het mogelijk voor een entiteit om het goed genoeg te doen, en dat de entiteit zekerheid geboden kan worden dat het niet aan vergaande vormen van toezicht onderworpen zal worden?

Ad 1: Zorgen over ondernemerszekerheid

De uitwerking van de Cbw laat heel veel details open voor nadere uitwerking. In bijlage 1 van deze brief hebben we een overzicht gemaakt van de punten die open zijn gebleven voor uitwerking via AMvB's. Dit maakt het vrijwel onmogelijk om de Nederlandse wet te beoordelen op zaken als impact en harmonisatie met andere landen. Dit schaadt de ondernemerszekerheid in Nederland en daarmee het vestigingsklimaat.

Wij begrijpen dat de Europese Unie hier ook een rol in heeft, omdat ook zij traag zijn met het uitwerken van enkele zeer essentiële zaken (met name de uitwerking van de *implementing act* ten behoeve van artikelen 21 en 23 van de NIS2). Maar zelfs als we dat in ogenschouw nemen, is de Nederlandse uitwerking meer een wetgevingskader dat concretisering voor zich uitschuift.

Het kan niet zo zijn dat ondernemingen na aanname van de Cbw nog steeds niet weten waar ze aan toe zijn, en waar ze op beoordeeld gaan worden. Want dat laatste is wat de onzekerheid veroorzaakt: ondernemingen uit de digitale sector zijn sinds jaar en dag met cybersecurity bezig, ze hebben zekerheid nodig om te weten of hun activiteiten ook voldoende invulling geven aan deze wet.
Het is momenteel onmogelijk om daar een uitspraak over te doen op basis van deze wet.

Wat hier bovendien aan bijdraagt is de uitspraak in de Memorie van Toelichting (p. 22): *'In de amvb wordt naar verwachting gebruik gemaakt van deze ruimte uit de richtlijn om maatregelen vast te stellen die een hoger cyberbeveiligingsniveau waarborgen.'*

Aangezien deze uitspraak niet verder gekwalificeerd wordt, lijkt hiermee de ambitie uitgesproken te worden om Nederlandse bedrijven aan hogere eisen te laten voldoen dan bedrijven uit andere lidstaten van de EU. De digitale sector is een internationale sector. Wij pleiten daarom voor grote inzet op geharmoniseerde wetgeving, dat versterkt de interne markt en is goed voor het Nederlandse vestigingsklimaat.

Op basis van voorgaande hebben wij de volgende concrete oproepen:

1. Scherp de Cbw verder aan door AMvB's in te kaderen voor de doeleinden waarvoor ze bedoeld zijn. Maak duidelijk wat organisaties kunnen verwachten. In de bijlagen bij deze brief staan meerdere punten benoemd waar dit nagelaten is, wat leidt tot grote onzekerheid over de reikwijdte van deze wetgeving.

2. Maak voor alle AMvB's inzichtelijk wanneer deze in concept verwacht zijn, wanneer ze geconsulteerd worden en met welke ambitie deze geschreven worden. Het is hierbij ook van belang dat deze data reëel zijn en niet tot op de rand van de implementatie verschoven worden.

3. Leg vast dat toezichthouders publiek communiceren hoe zij hun taken oppakken. Want de handhaving gaat direct in zodra de Cbw in werking treedt, ook als bedrijven door traagheid van de overheid geen tijd hebben gehad zich gedegen voor te bereiden. Hanteer daarbij de insteek dat wie al goed bezig is adviezen kan krijgen van de toezichthouder, en strenge handhaving in eerste instantie alleen plaatsvindt als organisaties nog helemaal geen actie hebben ondernomen.

4. Werk met andere Europese landen aan gezamenlijke eisen, maak die harmonisatie zichtbaar en laat die aansluiten bij bewezen internationale standaarden en normen. Laat de Europese markt echt één markt zijn, waarin een Nederlands bedrijf niet aan andere eisen moet voldoen dan een bedrijf uit andere lidstaten, zoals aangekondigd lijkt te worden in de Memorie van Toelichting. Dit zou ook mooi aansluiten bij het hoofdlijnenakkoord van de nieuwe regeringscoalitie, waarin onder 'Economie en vestigingsklimaat' is opgenomen *"Geen nieuwe nationale koppen op Europees beleid"* (pagina 25).

5. Ook als Nederlandse overheid, CSIRTs en toezichthouders zelf geen standaarden willen maken, dan kan er gekeken worden welke standaarden invulling geven aan (een deel van) NIS2-vereisten en kan dit proactief gecommuniceerd worden. Kijk naar voorbeelden als het Belgische Cyber Fundamentals (CyFun) en de Nederlandse Cyber Rating (CYRA) hoe eisen aan entiteiten concreet gemaakt kunnen worden. Denk hierbij ook aan de bekende standaarden als ISO27001 en SOC2.

Ad 2: Zorgen over gebrek harmonisatie binnen Nederland en stapelingen van plichten

Alhoewel de Cbw verwijzingen naar andere wetten bevat, mist integraal overzicht. Er komt veel op de digitale sector af aan wetgeving en het is belangrijk om oog te hebben voor het feit dat dit tot grote overlap kan leiden. Het betreft hier met name de details van de zorgplicht en stapeling van meldplichten.

Een concreet voorbeeld dat zeer reëel is: een leverancier die een combinatie levert van product en *software-as-a-service*, waar een incident plaatsvindt waarbij persoonsgegevens en financiële instellingen betrokken zijn. Deze zal vervolgens (vanaf 2026) te maken krijgen met meldingen onder de AVG, NIS2, DORA en CRA die ook bij toezichthouders én CSIRTs én ENISA moeten komen. Tijd is kostbaar tijdens cyberincidenten. Zeker in de eerste dagen na het incident waarin de spreekwoordelijke brand geblust moet worden. Tijdens een incident is de kennis nodig van de brandweerlieden die de cyberbrand moeten blussen, maar die moeten dan ook ongeveer 7

meldingen onder tenminste 4 wetten uitwerken. Dit meldproces moet gestroomlijnd worden om te voorkomen dat kostbare tijd verloren gaat aan onnodig veel vereiste administratieve handelingen.

De sectorale aanpak van de NIS2 heeft ook enkele valkuilen die ons zorgen baren. Niet alleen harmonisatie met andere EU-landen is een noodzaak, ook harmonisatie binnen Nederland verdient meer aandacht. Met een eigen CSIRT en eigen toezichthouder voor iedere sector kan dit voor een web aan uiteenlopende eisen zorgen. Het is belangrijk dat we in het oog houden waar het om gaat: meer veiligheid. Het gelijktrekken van eisen (voor zover dit haalbaar is) en het hanteren van een vergelijkbare toetsing zijn noodzakelijk om naleving voor leveranciers haalbaar te houden. De in de Memorie van Toelichting opgenomen tekst is op dit punt te zwak.

Dit brengt ons tot de volgende concrete oproepen:

1. Harmoniseer de enorm uiteenlopende wetgeving met elkaar. Beperk het aantal verschillende meldingen, met name gedurende incidenten. Breng meldplichten zoveel mogelijk met elkaar in lijn, en wanneer vergelijkbare informatie gevraagd wordt, laat die dan ook op dezelfde manier of via hetzelfde platform uitgevraagd worden. Luxemburg heeft op dit vlak reeds ervaring opgedaan.

2. Bouw meer waarborgen in om de wet niet in iedere sector tot andere interpretaties te laten komen. Het kan wenselijk zijn om hiertoe bijvoorbeeld de Rijksinspectie Digitale Infrastructuur een meer coördinerende rol te geven ten opzichte van alle betrokken toezichthouders.

Ad 3: Zorgen over toezicht – kan een bedrijf het goed genoeg doen?

Op het vlak van toezicht en handhaving hebben wij nog veel vraagtekens. Met name voor essentiële bedrijven springen artikelen 68, 69 en 70 in het oog: dit lijken zeer vergaande toezichtsmaatregelen die ook aan entiteiten die goed bezig zijn opgelegd kunnen worden.

Ten eerste is het niet duidelijk wanneer deze maatregelen ingezet kunnen worden, of er een aanleiding vereist is, en zo ja, welke aanleiding de inzet van deze maatregelen rechtvaardigt. Daarnaast is het zo dat een bedrijf dat al zeer hard werkt aan cybersecurity en op meerdere manieren audits en certificeringen heeft laten uitvoeren, volgens deze wet nog steeds een controlefunctionaris met nader te bepalen opdracht kan krijgen en een extra audit kan moeten laten uitvoeren. Het is onwenselijk dat een bedrijf dat goed bezig is en dit kan aantonen vervolgens al die zaken moet overdoen, en dan ook nog voor de kosten moet opdraaien.

Dit raakt ook zeer aan het eerste punt in onze inbreng: een bedrijf dat het goed doet zou zeker moeten kunnen zijn dat het niet aan dergelijke ingrijpende maatregelen zal worden blootgesteld. Het valt op dat deze wet in meerdere artikelen de ruimte neemt om de kosten voor toezicht naar entiteiten te verleggen die niets verkeerd gedaan hebben. Dit maakt zakendoen in Nederland een zeer onzekere aangelegenheid: je weet immers nooit wanneer de toezichthouder langskomt om extra kosten in rekening te brengen, en wat die kosten gaan zijn. Daar is geen begroting op te schrijven.

Tot slot gaat de escalatie in artikel 74 erg snel. Een route zou moeten beginnen met een waarschuwing, daarna een mogelijkheid tot escaleren naar bijvoorbeeld artikel 72 en pas daarna de mogelijkheid om artikel 74 toe te passen. De ruimte in de huidige bewoording van artikel 74 lid 2 staat echter een vrijwel directe escalatie toe.

Dit leidt tot de volgende concrete oproepen:

1. Maak duidelijk wanneer de maatregelen kunnen worden ingezet.

2. Beperk de controlefunctionaris (artikel 68) beveiligingsscan (artikel 69) en gerichte audit (artikel 70) al bij wet tot een sanctie die volgt op een waarschuwing waar geen (afdoende) gehoor aan gegeven wordt, of maak het mogelijk bestaande audits of certificeringen hiervoor aan te voeren.

3. Beperk in de wet dat kosten voor handhaving alleen naar de entiteit verlegd worden wanneer daar een aanleiding voor is. Beperk de willekeur aan onvoorspelbare kosten die deze conceptwet mogelijk maakt.

4. Pas artikel 74 lid 2 aan tot '[...] nadat zij twee of meer van de in het derde lid genoemde maatregelen [...]', zodat een waarschuwing en andere heftige maatregel altijd voorafgaan aan deze escalatie van handhaving.

Bijlage 1: Alle AMvB's op een rij

- Artikel 3: regels ter uitvoering van de op grond van de NIS2-richtlijn vastgestelde uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren.
- Artikel 17 lid 1: aanwijzing van sectorale CSIRTs.
- Artikel 18 lid 1: aanwijzing coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden en coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden.
- Artikel 23 lid 4: regels voor zorgplicht maatregelen (NIS2 21.2, CBW 23.1), waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en type entiteiten.
- Artikel 24 lid 3: regels ter uitvoering van de richtsnoeren van de EC over sectorspecifieke rechtshandelingen (bijvoorbeeld DORA) waardoor relevante bepalingen van de NIS2 wat betreft zorgplicht niet meer van toepassing kunnen zijn voor entiteiten.
- Artikel 26 lid 6: regels over de training van bestuur van entiteit (o.a. duur en niveau).
- Artikel 33 lid 3: regels ter uitvoering van de richtsnoeren van de EC over sectorspecifieke rechtshandelingen (bijvoorbeeld DORA) waardoor relevante bepalingen van de NIS2 wat betreft meldplicht niet meer van toepassing kunnen zijn voor entiteiten.
- Artikel 37: nadere regels worden gesteld ter uitwerking van de artikelen 27 tot en met 32, 35 en 36, waaronder regels over aanvullende aspecten en drempelwaarden die in aanmerking worden genomen om te bepalen of sprake is van een significant incident, waarbij onderscheid kan worden gemaakt tussen sectoren en subsectoren, en de gegevens waar de vroegtijdige waarschuwing, melding, tussentijds verslag en eindverslag in ieder geval uit moeten bestaan en de wijze waarop dit geschiedt.
- Artikel 45 lid 1 sub e: aanvullende informatie met betrekking tot informatieplicht ten behoeve van nationale register.
- Artikel 45 lid 3: regels over wijze van informatieverstrekking met betrekking tot informatieplicht ten behoeve van nationale register.
- Artikel 52 lid 2 sub a: mogelijkheid tot aanwijzen rechtshandhavingsautoriteiten die betrokken zijn bij samenwerking en informatie-uitwisseling.
- Artikel 52 lid 2 sub h: mogelijkheid tot aanwijzen bevoegde autoriteiten ten behoeve van sectorspecifieke EU-wetgeving die betrokken zijn bij samenwerking en informatie-uitwisseling.
- Artikel 64a lid 2: regels over de verwerking van bijzondere persoonsgegevens ten behoeve van taken CSIRT en de bevoegde autoriteit.
- Artikel 68 lid 3: mogelijkheid tot het omschrijven van gevallen waarbij de handhavingskosten van de controlefunctionaris niet voor rekening komen van de essentiële entiteit.
- Artikel 68 lid 4: overige regels over de controlefunctionaris, waaronder de vereisten voor aanwijzing.
- Artikel 69 lid 2: mogelijkheid om kosten voor uitvoeren beveiligingsscan te verplaatsen naar entiteit.
- Artikel 70 lid 4: mogelijkheid tot het omschrijven van gevallen waarbij de handhavingskosten van de gerichte beveiligingsaudit niet voor rekening komen van de essentiële entiteit
- Artikel 70 lid 6: overige regels over gerichte beveiligingsaudit voor essentiële entiteiten.
- Artikel 70a lid 3: overige regels over ad hoc beveiligingsaudit voor essentiële entiteiten.
- Artikel 79: mogelijkheid kosten beveiligingsscan te verleggen naar belangrijke entiteit.
- Artikel 80 lid 4: mogelijkheid tot het omschrijven van gevallen waarbij de handhavingskosten van de gerichte beveiligingsaudit niet voor rekening komen van de belangrijke entiteit
- Artikel 80 lid 5: overige regels over gerichte beveiligingsaudit voor belangrijke entiteiten.
- Artikel 89: aanpassing Telecommunicatiewet om daar cybersecuritymaatregelen in te kunnen opleggen via AMvB.

Bijlage 2 – opmerkingen per artikel

Artikel 1

- T.a.v. definitie ‘entiteit’ en samenhang met overweging 16 NIS2:
  - het is onduidelijk hoe dit gelezen moet worden als het gaat om een holding met verschillende werkmaatschappijen. Als een verbonden of partneronderneming onafhankelijk is van de entiteit, kan het zijn dat deze onderneming niet meegenomen wordt in de telling voor de omvang van de entiteit. Hoe wordt deze onafhankelijkheid bepaald? Wat wordt gezien als voldoende infrastructuurscheiding? Bijvoorbeeld layer 3 segmentatie (met afzonderlijke fysieke onderliggende netwerken)? Of duidt het meer op scheidingen op het niveau van applicatie, beheer, opslag etc.?

Artikel 2

- T.a.v. 2.1.a:
  - De term 'informatiesystemen' in de context van deze wet is niet gedefinieerd. Bedoelt men inderdaad 'geautomatiseerde informatiesystemen' of 'ICT-systemen'? Of wellicht "*toepassingen, diensten, informatietechnologische bedrijfsmiddelen of andere gegevensverwerkende componenten*" (ISO 27000)?
  - De term 'risico' in de context van deze wet is niet gedefinieerd.

Artikel 4

- T.a.v. 4.1.a:
  - Geldt dit ook voor in Nederland gevestigde holdingmaatschappijen die eigenaar zijn van werkmaatschappijen in meerdere EU-lidstaten (waaronder al dan niet Nederland)? Of geldt dit specifiek voor die werkmaatschappijen (voor zover die in Nederland gevestigd zijn)?

- T.a.v. 4.1.b:
  - Wordt hier gedoeld op "in Nederland gevestigde entiteiten die domeinnaamregistratiediensten verlenen" of op "entiteiten die domeinnaamregistratiediensten in Nederland verlenen", of wellicht op beiden, of wordt er iets anders bedoeld?

- T.a.v. 4.3:
  - De betekenis van dit artikellid is onduidelijk. Geldt er voor deze IT-sectoren geen omvangscriterium? Wat betekent dit voor bedrijven uit deze sectoren die niet belangrijk of essentieel zijn? Of is het slechts de bedoeling geweest om voor de entiteiten in artikel 4 lid 3 een *one stop shop* mechanisme te creëren (dat voor die entiteiten maar één implementatiewet geldt, namelijk de Nederlandse, en dus ook maar één registratieplicht, één toezichthouder etc)? In alle gevallen is verdere verheldering van dit artikellid gewenst.
  - Het rijtje entiteiten in lid 3 strookt niet helemaal met artikel 26 lid 1 sub b NIS2. In Cbw staat ‘aanbieders van datacentrumdiensten’ en in NIS2 staat ‘aanbieders van datacentra'.
  - Daarbij de vraag of dit artikellid ook geldt voor in Nederland gevestigde holdingmaatschappijen of alleen specifiek voor werkmaatschappijen (voor zover die in Nederland gevestigd zijn).

- T.a.v. 4.4:
  - Definitie van ‘hoofdvestiging’ wijkt kennelijk af van de Handelsregisterwet: "het door een onderneming als zodanig aangemerkte onderdeel van de onderneming" (artikel 1 lid 1 sub k Hw). De definitie wijkt ook (deels) af van de definitie in de AVG (artikel 4 sub 16).
  - met betrekking tot de bewoording van het artikel: *‘[...] wordt de hoofdvestiging geacht zich in Nederland te bevinden indien de cyberbeveiligingsactiviteiten in Nederland worden uitgevoerd. Indien niet kan worden bepaald in welke lidstaat de cyberbeveiligingsmaatregelen worden uitgevoerd [...]’* > blijf dezelfde term gebruiken. Zie ook artikel 26 lid 2 NIS2, waar ‘cyberbeveiligingsactiviteiten' wordt gebruikt.

Artikel 8

- T.a.v. 8.1:
  - Bijlage 1 en bijlage 2 bij de Cyberbeveiligingswet komen niet letterlijk overeen met bijlage 1 en bijlage 2 bij de NIS2. De definities uit die bijlagen (rechtstreeks uit NIS2 richtlijn) zijn uitgebreider en completer dan wat nu in de Cyberbeveiligingswet staat. Dat zorgt voor onduidelijkheid. Waarom houdt de wetgever niet de letterlijke NIS2 definities aan met evt. NL specifieke uitbreidingen/uitzonderingen?

Artikel 15

- In dit artikel wordt de Minister van Justitie en Veiligheid aangewezen als centraal contactpunt. Wij benadrukken hierbij graag dat het gewenst is dat het centrale contactpunt aandacht heeft voor het versterken van de cyberweerbaarheid en samenwerking met het bedrijfsleven. Wij roepen op tot een aanpak die samenwerking als uitgangspunt neemt.

Artikel 16

- Wie is autoriteit bij competentie-overschrijdende zaken? Bijvoorbeeld een ICT-incident bij een voedselproducent of drinkwaterleverancier?

Artikel 17

- T.a.v. 17.2.e:
  - Is dit niet een markttaak? Wat zijn waarborgen dat overheid hierop niet de Wet Markt en Overheid overtreedt? Een alternatief door de markt moet mogelijk zijn. Verduidelijking is gewenst met betrekking tot onder welke voorwaarden scans die zijn uitgevoerd c.q. bij een derde partij ingekocht door de entiteit een acceptabel alternatief zijn voor scans door de CSIRT.

- T.a.v. 17.3:
  - Hoe weet een CSIRT zeker dat haar scans niet intrusief zijn, en als ze onbedoeld wel intrusief blijken, komt dit dan niet neer op computervredebreuk, waarvoor de gescande entiteit vooraf een vrijwaring aan de CSIRT moet afgeven?

- T.a.v. 17.4:
  - Ook hier geldt: is dit niet een markttaak? Wat zijn waarborgen dat overheid hierop niet de Wet Markt en Overheid overtreedt?

Artikel 20

- T.a.v. 20.3:
  - In hoeverre volgen uit de nationale cyberbeveiligingsstrategie extra verplichtingen voor de entiteiten die aan deze Cyberbeveiligingswet moeten voldoen? Met andere woorden, moet deze clausule worden gelezen als een 'ISO27001 Annex A'-achtige constructie?

Artikel 22

- T.a.v. 22.1:
  - (Hoe) kunnen entiteiten het nationaal register raadplegen om hun registratie daarin te controleren/corrigeren?
  - Samenhang met andere wetgeving: wordt ditzelfde register ook gebruikt voor entiteiten die als kritische/essentiële/belangrijke entiteit worden aangemerkt vanuit de Wwke en eventueel de DORA?

Artikel 23

- T.a.v. 23.3:
  - De term 'gevaren' is niet gedefinieerd, dat leidt tot onduidelijkheid. Uit de MvT blijkt daarnaast dat het gaat om zowel gebeurtenissen met kwade wil als gebeurtenissen zonder kwade wil. Dit kan worden verduidelijkt in de wettekst. Naast een definitie van gevaren, kan ‘alle gevaren’ bijvoorbeeld aangevuld worden met ‘per ongeluk of onrechtmatig’ (naar analogie van artikel 4 sub 12 AVG over datalekken).

Artikel 26

- T.a.v. 26.1:
  - Een eenduidige definitie van 'bestuur'/'bestuurder' in deze context ontbreekt. Gaat het over (de leden van) het bij de KvK ingeschreven 'C-level' / 'raad van bestuur' zoals de NIS2 suggereert, of over alle managers in de organisatie, of iets anders?

- T.a.v. 26.2 sub a, b en c:
  - in de meeste (grotere) entiteiten zal dit bij gespecialiseerde functionarissen/afdelingen belegd zijn. Wat is de precieze reikwijdte en diepgang van de betrokkenheid van het bestuur bij risico-identificatie en -beoordeling?

- T.a.v. 26 lid 2 en 3:
  - Deze artikelen in samenhang lijken te zeggen dat ieder bestuurslid binnen twee jaar na inwerkingtreding van de wet over de vereiste kennis en vaardigheden beschikt (of binnen twee jaar na benoeming). In de MvT (p. 23) staat echter dit: *‘Nieuwe bestuursleden moeten kunnen aantonen dat de training binnen twee jaar na hun benoeming gevolgd is (artikel 26, derde lid, van dit*

wetsvoorstel). Voor zittende bestuursleden geldt dat zij een relevante training moeten hebben gevolgd binnen twee jaar nadat artikel 26, tweede lid, van dit wetsvoorstel in werking is getreden (artikel 26, derde lid, van dit wetsvoorstel). Wel rust op hen vanaf de inwerkingtredingsdatum de verplichting dat zij over voldoende kennis en vaardigheden beschikken. Het is aan het bestuurslid om aan te tonen dat hiervan sprake is.' Dat laatste lijkt logisch, maar dat wordt niet duidelijk uit de huidige bewoording van artikel 26.

- T.a.v. 26.2, 26.4 en 26.5:
  - Graag meer duidelijkheid over de eisen waaraan de training en het certificaat moeten voldoen. Zonder verdere kaders zorgt dit voor een wildgroei aan opleidingen en trainingen waarbij de kwaliteit niet is gegarandeerd. Dan schiet deze bepaling zijn doel voorbij. En kan een eigen/interne opleiding/training, bijvoorbeeld door de beheerder van het daartoe ingerichte Information Security Management System (ISMS), ook voldoen?

Artikel 27

- Zonder duidelijke definitie van 'significante incidenten' zijn deze bepalingen niet te beoordelen. Met name de toevoeging 'kan veroorzaken' is een te open norm; in theorie 'kan' bijna alles een dergelijke verstoring veroorzaken, maar het gaat juist om de situaties waarbij zich dit ook daadwerkelijk voordoet. Een overvloed aan '*false positives*' zorgt voor een overbelasting van de relevante autoriteiten, waardoor een daadwerkelijk ernstig significant incident niet wordt opgepakt (het zogenaamde "*boy who cried wolf*" scenario).

- 'Een incident is volgens deze bepaling een significant incident als het een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken': gaat het hierbij om 'ernstige financiële verliezen'? Of is er bij elk financieel verlies, ongeacht de grootte/ernst, al sprake van een significant incident? Dat lijkt onwenselijk. En als vervolgvraag: wanneer kwalificeert iets als 'ernstig of 'aanzienlijk'?

Artikel 28

- T.a.v. 28.2.b:
  - de definitie van 'grensoverschrijdend' ontbreekt. Wordt hiermee bijvoorbeeld buiten de EU/EER of buiten Nederland bedoeld?

Artikel 29

- T.a.v. 29.1.b:
  - wordt er duidelijkheid/richtlijnen gegeven om de ernst te bepalen?

- T.a.v. 29.1.d:
  - wordt er duidelijkheid/richtlijnen gegeven welke informatie doorgaans vereist is om de grensoverschrijdendheid te bepalen (en wat dus onder 'alle beschikbare informatie' kan vallen)? Nadere uitleg is gewenst.

Artikel 32

- Verhouding met AVG: komt niet volledig overeen met de plicht tot het informeren van betrokkenen onder de AVG (artikel 34). Kan tot onduidelijkheid leiden. En gelden de meldplichten ook in de volgorde uit de AVG? Dus eerst de toezichthouder en dan de betrokkenen? En geldt de informatieplicht richting derden ook voor niet-significante incidenten die de melddrempel niet overschrijden?

- T.a.v. artikel 32.1:
    - dit artikellid moet zodanig worden aangescherpt dat duidelijk is dat klanten alleen geïnformeerd moeten worden over incidenten die de door hen afgenomen diensten raken. Overbodige notificaties moeten namelijk voorkomen worden (notificatie-moeheid). De huidige bewoording kan zo worden gelezen dat klanten ook meldingen moeten krijgen over incidenten bij diensten die zij niet afnemen (omdat zij andere diensten afnemen van de entiteit dan de dienst waar zich een incident heeft voorgedaan).

Artikel 35

- Hoewel vanuit moreel opzicht het melden van alles dat relevant is bijdraagt aan cyberveiligheid van de maatschappij, zal de dreiging van reputatieschade, bestraffing en de kosten van inspanning mogelijk blokkerend kunnen werken. Kunnen hier waarborgen voor worden ingeregeld?

- T.a.v. 35.1:
    - Hoe worden foutieve/valse meldingen gedetecteerd en afgehandeld?

Artikel 36

- T.a.v. 36.1:
    - Hoe worden (anonieme) foutieve/valse meldingen gedetecteerd en afgehandeld?

Artikel 38

- T.a.v. 38.3:
    - In de bepaling staat ‘wanneer wordt vermoed dat...’: wie moet dit vermoeden? Het CSIRT of de entiteit? Of kan het allebei? Kijkt het CSIRT proactief of het vermoedt dat het incident van criminele aard is, of kijkt het daar alleen maar naar als de entiteit dit aangeeft?

Artikel 39

- Het is onduidelijk wanneer het CSIRT het publiek moet informeren, er moeten voor entiteiten ruime mogelijkheden zijn voor inspraak en het in bezwaar gaan tegen openbaarmaking. Dit zou alleen in zeer uitzonderlijke gevallen ongecoördineerd mogen gaan.

Artikel 42

- Als een entiteit aparte meldingen doet onder de Cyberbeveiligingswet en onder de Wwke, worden deze dan gelinkt als het over dezelfde kwetsbaarheid/hetzelfde incident gaat? En wordt informatie over Wwke-meldingen ook gedeeld met NIS2-toezichthouders en de CSIRT?

Artikel 43

- T.a.v. 43.1:
  - Het doorsturen naar een CSIRT of een bevoegde autoriteit lijkt willekeurig (door het woord ‘kan'): wanneer wordt de informatie naar wie doorgestuurd?

Artikel 45

- T.a.v. 45.1:
  - Werkbaarheid is onduidelijk. Denk bijvoorbeeld aan 45.2 in relatie tot IP-adressen en e-mailadressen in 45.1.b. Moet een dergelijk bedrijf bijvoorbeeld iedere personeelswijziging melden binnen twee weken omdat er een nieuw of verlopen mailadres is? En hoe kom je achter je IP-adressen als alle ICT is uitbesteed en je aanbieder niet alle informatie wil verstrekken vanwege veiligheidsredenen?
  - Mogen dit ook algemene contactgegevens zijn (denk hierbij aan een initiatief als security.txt e.d.)? Voor personeelswijzigingen op sleutelposities is het misschien nog wel te overzien, maar wanneer iemand bijvoorbeeld met verlof is wil je dat niet iedere keer moeten doorgeven.
  - Waarom IP-bereiken verstrekken als die al in openbare registers worden bijgehouden (zie art. 50)? Dubbele registratie levert extra administratieve lasten op die vermijdbaar lijken. Of wordt i.p.v. IP-bereiken de domeinnaam bedoeld (ofwel de 'www pagina')?

- T.a.v. 45.1.c:
  - Waarom hier niet de KvK registers gebruiken? Dubbele registratie levert extra administratieve lasten op die vermijdbaar lijken.

Artikel 48

- T.a.v. 48.2:
  - Gaat dit gecombineerd met algemene informatieplicht (artikel 45)? Het is onwenselijk om dubbel te moeten doen.

- T.a.v. 48.3:
  - Betekent dit dat werkmaatschappijen individueel moeten 'inschrijven', ook al vallen ze onder een gemeenschappelijke 'holding'?

Artikel 50:

- T.a.v. 50.5:
  - Er staat ‘verlemem’ ipv ‘verlenen’

Artikel 52

- T.a.v. 52.2:
  - Als een entiteit aparte inschrijvingen/meldingen doet onder de Cyberbeveiligingswet en onder de Wwke en andere wetgeving, hoe worden deze dan gelinkt als het over dezelfde entiteit gaat? Waarom geen centraal register over de verschillende wetten/ministeries heen, om administratieve overhead te beperken?
  - Hoe wordt de privacy geborgd als persoonsgegevens zo worden gedupliceerd? Is daar niet het minimalisatieprincipe volgens de AVG op van toepassing?

Artikel 53

- Zelfde commentaar als bij artikel 52.

Artikel 54

- Er staat 'deentiteiten' ipv 'de entiteiten' (en een dubbele spatie)
- Er staat NIS@ richtlijn ipv NIS2

Artikel 55

- Zelfde commentaar als bij artikel 52.
- Is “derde landen” niet een te ruim begrip? Moet dit niet worden beperkt tot EU/EER-landen?

Artikel 57

- T.a.v. 57.1.a:
  - Worden deze registers geïntegreerd of gesynchroniseerd? Wat gebeurt er bij discrepanties tussen losse registers?

Artikel 59

- T.a.v. 59.2:
  - wat gebeurt er als de doorgifte via de bevoegde autoriteit aan de AP afwijkt qua inhoud of timing van de directe melding door de entiteit aan de AP?
  - Er staat Autoriteit persoonsgegevens (kleine letter p) ipv Autoriteit Persoonsgegevens (ook in artikel 52 lid 2 sub b)

Artikel 64a

- Hoe kunnen betrokkenen, waarover in het kader van deze wet persoonsgegevens worden verwerkt, hun rechten volgens de AVG uitoefenen?

Artikel 65

- T.a.v. 65.1.d:
    - Hoe kan de entiteit vaststellen dat dit effectief gebeurt? M.a.w. dat diens gegevens over personen en kwetsbaarheden niet 'op straat liggen'?

Artikel 68

- Art. 68-70 leggen veel macht/verantwoordelijkheid bij één instantie. Dit kan mogelijk leiden tot wachtrijen en oneerlijke concurrentie met bedrijven. Het verdient de voorkeur om criteria vast te leggen voor een scan/audit of hier eventueel certificering voor te maken

- T.a.v. 68.1:
    - Onduidelijk wat de aanleiding voor het aanwijzen van een controlefunctionaris is, en of er een aanleiding nodig is. Hoe werkt dit (zeker omdat je blijkbaar zelf voor kosten opdraait (zie 68.3))?

- T.a.v. 68.2:
    - De controlefunctionaris is, volgens dit artikel, een onafhankelijke deskundige. Onduidelijk is wat de status van deze functionaris is. Welke kwalificaties en ethische gedragsnormen moet de controlefunctionaris hebben? Zou dit -zoals bij een Functionaris Gegevensbescherming- ook een eigen medewerker kunnen zijn? De onafhankelijke status van deze medewerker zou wettelijk en contractueel vastgelegd kunnen worden, zoals bijvoorbeeld wettelijke ontslagbescherming en contractuele geheimhouding. Als een externe partij op kosten van de entiteit zou moeten worden ingehuurd dan zou dit een aanzienlijke belasting betekenen; de ervaring leert dat dergelijke partijen niet voor het aangegeven uurtarief van €60,- te vinden zijn. Daarnaast zal deze functionaris samenwerken en input nodig hebben van andere medewerkers van de organisatie, die zich daarvoor ook moeten inzetten en een uurtarief hebben. Ook dit brengt voor de entiteit aanzienlijke kosten met zich mee.

- T.a.v. 68.3:
    - Is het gangbaar dat het bedrijf moet betalen voor onder toezicht staan zonder aanleiding? Hoe wordt proportionaliteit in acht genomen? Als er geen aanwijsbaar verwijtbare reden is, is dit dan geen blanco cheque? In sommige contracten wordt afgesproken dat de klant een right-to-audit heeft, waarbij de klant de kosten draagt, tenzij wordt aangetoond dat de leverancier in gebreke is. Dat zou hier mogelijk ook kunnen werken (mits de toetsingsnormen verduidelijkt worden).

Artikel 69

- T.a.v. 69.1:
    - Onduidelijk in welke omstandigheden dit gebeurt en hoe de noodzaak wordt vastgesteld
    - Volgens deze bepaling mag de bevoegde autoriteit een beveiligingsscan uitvoeren. Dergelijke scans worden normaal gesproken door commerciële partijen aangeboden. Als de bevoegde autoriteit deze ook zelfstandig gaat uitvoeren werkt dit mogelijk marktverstorend. Ook dienen dergelijke scans tijdig te worden aangekondigd, zodat de security organisatie (SOC) van een entiteit hiervan op de hoogte is en onnodige beveiligings(tegen)maatregelen worden voorkomen.

- Hoe weet de bevoegde autoriteit zeker dat haar beveiligingsscans niet intrusief zijn, en als ze onbedoeld wel intrusief blijken, komt dit dan niet neer op computervredebreuk, waarvoor de gescande entiteit vooraf een vrijwaring aan de uitvoerder van de scan moet afgeven?

- T.a.v. 69.2:
  - Dit geeft erg veel ruimte aan minister om het om te draaien en brengt daarmee onzekerheid. Deze gegeven ruimte vraagt om meer doel-binding.

Artikel 70

- T.a.v. 70.1:
  - In welke omstandigheden worden zulke audits gehouden en wat is de notificatie periode? Kan dit zonder enige vooraankondiging plaatsvinden?

- T.a.v. 70.2:
  - Een door de bevoegde autoriteit verrichte risicobeoordeling is een 'dat vullen we later nog wel in' clausule. Daar kunnen entiteiten qua naleving dus niet op richten. E.e.a. zou gelijktijdig met de wet duidelijk moeten zijn.

- T.a.v. 70.3:
  - ook dit is een 'dat vullen we later nog wel in' clausule. Daar kunnen controlefunctionarissen qua naleving dus niet op richten. E.e.a. zou gelijktijdig met de wet duidelijk moeten zijn.

- T.a.v. 70.4:
  - Zelfde commentaar als bij 68.3

- T.a.v. 70.6:
  - in de concepttekst staat 70.6 maar het moet waarschijnlijk 70.5 zijn.

Artikel 70a

- T.a.v. 70a.1.a:
  - welke kwalificaties en ethische gedragsnormen moet de deskundige hebben? Moet dat een RE zijn?

Artikel 71/81

- De NIS2-richtlijn beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken. Niet duidelijk is welk doel het openbaar maken van een overtreding heeft ten opzichte van het beoogde doel van de NIS2. Deze '*naming and shaming*' draagt niet bij aan het doel vooral van elkaar te leren en de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken. Het moet voor entiteiten mogelijk zijn om anoniem te blijven. Het kan onder bepaalde omstandigheden de markt juist verstoren ipv weerbaarder te maken. Daarnaast kan er (ook) een verdenking van een strafbaar feit meespelen, waar ook natuurlijke personen verdachten kunnen zijn. Dat botst met 2016/680 en de WPG/WJD. En het is ook nog eens een beschikking onder de Awb, en kan dus tot bestuurlijke procedures

leiden.

Artikel 74

- Hoe wordt de einddatum om de maatregelen om te zetten vastgesteld? Zeer onduidelijk hoe dit wordt vastgesteld.

- Het valt op dat artikel 74 al na een waarschuwing mogelijk is als escalatie, is het niet logischer om dan eerst artikel 72 in te zetten? Het is in dat opzicht verstandig uit te gaan van 2 maatregelen in plaats van één maatregel in lid 2 sub b.

Artikel 75

- Het is niet duidelijk wat hier bedoeld wordt. Gaat het dan b.v. om ISO27001, en de certificerende instantie te verzoeken die in te trekken? Het is niet duidelijk hoe dit werkt. Als een instantie aan certificeringseisen voldoet, maar in overtreding is volgens NIS2, kan dan toch zijn certificaat worden ingetrokken? Certificeringen, zoals ISO certificeringen, worden jaarlijks beoordeeld en hebben een bepaalde geldigheidsduur die op de certificaten zijn aangegeven. Of certificeringen binnen deze termijn zijn geschorst is voor een derde niet te zien. De praktische toepassing van deze bepaling is daarmee onduidelijk, dit artikel moet duidelijker.

Artikel 76

- T.a.v. 76.1:
  - Kunnen alle leden worden geschorst? Wat betekent dat in de praktijk? Dan stopt een gemiddeld bedrijf met functioneren omdat er geen legale vertegenwoordiging (algemeen) meer is.
  - Rijdt dit niet in de wielen van bijvoorbeeld de Ondernemingskamer bij private entiteiten? En voor overheden heeft de Kroon in de regel bevoegdheden tot schorsing van politiek bestuurders.

- T.a.v. 76.3:
  - levert dit geen financiële 'perverse prikkel' om de entiteit *non-compliant* te verklaren?
  - Wat is de verhouding tot de Awb en leerstukken uit het bestuursrecht over (mede)plegen van bestuurlijke overtredingen? En vooral over ‘feitelijk leidinggeven aan’?

- T.a.v. 76.5:
  - Bij voorkeur iets opnemen in de trant van dat de KvK de opname onverwijld verwijderd uit het Handelsregister

Artikel 77

- Komen er boetebeleidsregels?

Artikel 79

- T.a.v. 79.1:
  - Hoe weet de bevoegde autoriteit zeker dat haar beveiligingsscans niet intrusief zijn, en als ze onbedoeld wel intrusief blijken, komt dit dan niet neer op computervredebreuk, waarvoor de gescande entiteit vooraf een vrijwaring aan de uitvoerder van de scan moet afgeven?

- T.a.v. 79.2:
  - Zelfde commentaar als bij 69. Dit geeft erg veel ruimte aan minister om het om te draaien en brengt daarmee onzekerheid. Deze gegeven ruimte vraagt om meer doelbinding.

Artikel 80

- Over het auditrecht bestaat geen discussie, maar volgens deze bepaling komen alle kosten voor deze audit voor rekening van de entiteit. Graag in de AMvB krachtens artikel 80 lid 4 opnemen dat alleen bij een significante overtreding de kosten voor rekening van de entiteit dienen te komen. Ook zien we graag een tijdige aankondigen van een audit, omdat hiervoor aan de kant van de entiteit ook de juiste mensen beschikbaar moeten zijn. Graag op voorhand helderheid over de regels m.b.t. de audit. Hoe wordt bijvoorbeeld voorkomen dat een audit de bedrijfsvoering niet verstoord c.q. tot financiële schade lijdt?

- T.a.v. 80.2:
  - ook een door de bevoegde autoriteit verrichte risicobeoordeling is een 'dat vullen we later nog wel in' clausule. Daar kunnen entiteiten qua naleving dus niet op richten. E.e.a. zou gelijktijdig met de wet duidelijk moeten zijn.

- T.a.v. 80.3:
  - dit is een 'dat vullen we later nog wel in' clausule. Daar kunnen controlefunctionarissen qua naleving dus niet op richten. E.e.a. zou gelijktijdig met de wet duidelijk moeten zijn.

- T.a.v. 80.4:
  - dit is een 'dat vullen we later nog wel in' clausule. Daar kunnen entiteiten qua naleving dus niet op richten. E.e.a. zou gelijktijdig met de wet duidelijk moeten zijn.