Aan: Ministerie van Justitie en Veiligheid, demissionair Minister van Justitie en Veiligheid, Mw. D. Yeşilgöz–Zegerius

Betreft: Internetconsultatie implementatie NIS2-Richtlijn

Den Haag, 27 juni 2024

Excellentie,

Hierbij geeft De Dutch Cloud Community een reactie op de Internetconsultatie inzake oftewel Implementatiewet tot uitvoering van de Richtlijn (EU) 2022/2555[1] (hierna: Cyberbeveiligingswet). Wij zijn verheugd dat NIS2 er is en thans in Nederland metterdaad geïmplementeerd gaat worden. Voor deze reactie heeft DCC de Cyberbeveiligingswet inclusief de Memorie van toelichting (hierna MvT) alsmede de NIS2 Richtlijn (EU) 2022/2555 (hierna: NIS2-Richtlijn) gebruikt.

In deze brief vragen wij uw aandacht voor: de verantwoordelijkheid van de toeleveringsketen; de regeldruk en onbedoelde neveneffecten; kosten en prijs voor het gewenst beveiligingsniveau; ISO 27001 als richting voor ICT-dienstverleners; NIS2 als katalysator voor stimuleren van Dutch Cloud; de samenhang tussen NIS2 en andere (ICT) wetgeving; verwijzingen naar NIS2-Richtlijn; en de risico's van een versnipperd sectorale toezicht. In de bijlage zijn enkele artikelsgewijze commentaren en verzoeken opgenomen.

Ketenverantwoordelijkheid

In artikel 21, tweede lid, NIS2-richtlijn is bepaald dat de essentiële entiteiten en belangrijke entiteiten ook de toeleveringsketen moeten betrekken. NIS2 kent derhalve eisen en verplichtingen die doorwerken in de gehele ICT-keten. Die doorwerking leidt er toe dat door entiteiten aan gecontracteerde ICT-dienstverleners een bepaalde verantwoordelijkheid rondom cybersecurity toebedeeld zullen worden. DCC is verheugd dat er ook en vooral aandacht is voor de toeleveringsketen en streeft er naar dat haar leden ten aanzien van cybersecurity een bepaalde mate van verantwoordelijkheid in acht nemen. DCC stimuleert dat door awareness te creëren onder de leden en allerhande ondersteunende documentatie aan te reiken. Echter, DCC vraagt zich ook wel af hoever de verantwoordelijkheden en zorg(plichten) van de betrokken ICT-dienstverlener en de entiteit - zijnde de opdrachtgever – strekt en hoe die tussen elkaar interacteren. Waar ligt de scheidslijn? ICT-dienstverleners zijn bereid te helpen en aldus mee te denken met hun opdrachtgevers, maar worden ook vaak geconfronteerd met de technische, commerciële en juridische keuzes van een opdrachtgever en hoe opdrachtgever afgenomen diensten wenst te gebruiken.

DCC is van mening dat de verantwoordelijkheid ten aanzien van beveiliging een gedeelde verantwoordelijkheid is van ICT-dienstverlener en opdrachtgever. DCC stimuleert dat ICT-dienstverleners een sterke basis diensten leveren, en dat ze in samenspraak met bedrijven en overheden verantwoordelijkheid dragen voor het implementeren van hun systemen en het beveiligen van hun gegevens. In de Cyberbeveiligingswet zien we die gedeelde verantwoordelijkheid niet uitgewerkt. DCC vraagt u daarom in Cyberbeveiligingswet en/of de MvT

[1] Wetsvoorstel strekt tot de uitvoering van de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148.

expliciet op te nemen wat de onderlinge verantwoordelijkheden zijn van entiteiten en hun ICT-dienstverleners.

Regeldruk en onbedoelde neveneffecten

In de MvT staat in paragraaf 8 de regeldruk beschreven. Daarin staat onterecht dat het wetsvoorstel geen gevolgen heeft voor de regeldruk voor burgers en bedrijven die ofwel niet binnen de genoemde sectoren of categorieën vallen, ofwel de drempelwaardes niet overschrijden, ofwel niet anderszins bij besluit of regeling aangewezen zijn. Hier wordt onzes te snel voorbijgegaan aan het effect van NIS2 op de ICT-sector. DCC is van mening dat wel degelijk regeldruk ontstaat via de ketenverantwoordelijkheid en hoe de NIS2 regels contractueel kunnen doorwerken.

Entiteiten en ICT-leveranciers staan in toenemende mate in verbinding met elkaar, waardoor een risico's en daarmee ook de eisen kunnen doorwerken via keten-effecten binnen een sector, richting andere sectoren of over grenzen heen ('cross-border'). Ook door onbedoelde, negatieve neveneffecten van maatregelen kunnen risico's verlegd worden. DCC verzoekt u met klem de regeldruk en impact van NIS2 in kaart te (laten) brengen en welke technische en commerciële gevolgen dat heeft voor zowel de ICT-dienstverleners enerzijds en opdrachtgevers c.q. entiteiten anderzijds.

Kosten en prijs voor gewenst beveiligingsniveau

Het implementeren en onderhouden van cybersecurity maatregelen hebben vaak hoge en onverwachte kosten die aldus kunnen leiden tot een hogere prijs voor de dienstverlening van ICT-dienstverleners in dit kader. In de MvT wordt de financiële impact onderschat en wordt er onzes inziens onvoldoende ingegaan op het kostenaspect. Wij verzoeken u inzichtelijk te maken hoe NIS2 kostenverhogend (door)werkt op het te ontwikkelen beveiligingsniveau en de af te nemen ICT-dienstverlening. Sectoren zijn er bij gebaat dat er over kosten zomin mogelijk discussie ontstaat en dat de focus komt te liggen op het realiseren het gewenste beveiligingsniveau.

Standaardisatie: ISO 27001 als toetsingsmaatstaf

In de MvT staat dat de entiteiten hun eigen normenkader kunnen hanteren voor het beheersen van hun risico's ten aanzien van de beveiliging van netwerk- en informatiesystemen, waarbij de ISO/IEC 27000-serie als voorbeeld genoemd wordt. Juist omdat ICT-dienstverleners direct of indirect steeds meer aan verschillende eisen moeten voldoen om conformiteit voor hunzelf dan wel hun opdrachtgevers, kiezen ICT-dienstverleners ervoor om hun organisatie en dienstverlening te laten certificeren. Voor de ICT-sector zijn de juridische eisen die hen wettelijk en/of contractueel worden opgelegd niet te overzien. Daarom is het wenselijk dat er begrijpelijke kaders en normen worden geboden, waarin minimumeisen voor ICT-leveranciers staan. Zo ziet DCC graag dat in de Cyberbeveiligingswet wordt vastgelegd dat het voor ICT-dienstverleners het hebben van een ISO 27001 certificaat voldoende rechtsvermoeden is dat voldaan wordt aan NIS2. Op deze manier kan de ISO 27001 als een richting voor ICT-dienstverleners gehanteerd worden en gestimuleerd worden dat ten minste conform ISO 27001 gewerkt wordt, zodat ook eventuele aanvullende eisen maatwerk-eisen zijn die opdrachtgevers voor eigen rekening en risico voor kunnen kiezen.

NIS2 als katalysator voor Dutch Cloud

Op Kamervragen heeft de minister gezegd dat NIS2 of aanverwante wetgeving zoals de DORA Act geen expliciet voorkeursbeleid voor ICT-diensten (zoals clouddiensten) van

Nederlandse/Europese bodem betekent, maar dat Dutch of European Cloud wel wordt gestimuleerd.[2] Met NIS2 Richtlijn en andere aankomende wetgeving ligt er onzes inziens een kans om het gebruik van ICT-diensten van Nederlandse/Europese bodem te stimuleren. DCC pleit in dit kader voor richtlijnen die sneller kunnen leiden tot het kiezen voor Nederlandse aanbieders van Clouddiensten. Hiermee kan ook beter de gewenste strategische autonomie gerealiseerd worden.

Samenhang tussen NIS2 en andere (ICT) wetgeving

Er zijn verschillende Europese wetgevingskaders met een eigen set weerbaarheidsmaatregelen. ICT-dienstverleners worden geconfronteerd met verschillende sets juridische eisen die telekens weer een doorvertaling nodig hebben naar technische en organisatorische maatregelen. DCC verzoekt u duidelijker te maken hoe die verschillende wetgeving met elkaar samenhangt en vooral ook hoe op elkaar inwerken. Daarbij zien we graag de vraag beantwoord in hoeverre een ICT-dienstverlener met een ISO 27001 certificering in de basis al voldoet aan de verschillende ICT-wetgeving, en wat er eventueel nog aanvullend geregeld moet worden door betrokken partijen.

Verwijzingen naar NIS2-Richtlijn

Uit oogpunt van zelfstandige leesbaarheid en hanteerbaarheid van de Cyberbeveiligingswet verzoeken wij om niet in de Cyberbeveiligingswet te verwijzen naar artikelen, artikelleden en onderdelen van de Europese Richtlijn die van toepassing zijn, maar de van toepassing zijnde bepalingen zelf uit te schrijven in de Cyberbeveiligingswet en nader te expliciteren met concrete toepassingen.

Sectorale toezicht

Het feit dat de toezicht- en handhavingsverantwoordelijkheid voor cybersecurity belegd is bij verschillende partijen (NCTV, NCSC en het CSIRT-DSP, de RDI, AIVD) kan onzes inziens leiden tot een versnipperd beleid. DCC wenst daarom voor ICT-dienstverleners een duidelijk aanspreek- en meldpunt aan te wijzen opdat de ICT-sector haar verantwoordelijk effectief en efficiënt kan dragen. Wij begrijpen dat met een sectorspecifieke verdeling efficiënter en effectiever ingespeeld kan worden op de daadwerkelijke behoeften van een betreffende sector. Echter, voor de ICT-sector verzoeken wij u één partij als aanspreekpunt aan te wijzen, bijvoorbeeld de RDI.

Tot slot

DCC hoopt dat u onze aandachtspunten, verzoeken en adviezen mee wilt nemen in uw verdere uitwerking van de Cyberbeveiligingswet en is graag bereid nadere toelichting geven over onze reactie in dezen.

Hoogachtend,

Dutch Cloud Community

[2] Nota naar aanleiding van het verslag wetsvoorstel Implementatiewet digitale operationele weerbaarheid (DORA)

Bijlage: Artikelsgewijs commentaar

In deze bijlagen nog een aantal verzoeken en commentaar op verschillende artikelen in de Cyberbeveiligingswet.

Artikel/Onderwerp	**Commentaar/verzoek**
Administratieve last MKB	Kleine en micro bedrijven conform EU richtlijn vallen al snel onder de regelgeving en de administratieve (data) 'last' is onevenredig groot als gevolg daarvan. Ketenverantwoordelijkheid. Dit vertaalt zich ook in hogere kost voor eindklant. De verplichting tot audit brengt een dermate zware last met zich mee voor kleinere bedrijven dat hier mogelijk een deel van de DCC achterban soort van buiten de markt komt te staan.
Artikel 23	Zorgplicht-omschrijving is nu vaag en niet concreet als in art 21 NIS2-Richtlijn, dat een concreter lijst bevat. In het voorstel van wet (Cyberbeveiligingswet) wordt in artikel 23 wordt gesproken over "… passende en evenredige technische, operationele en organisatorische maatregelen om…", maar wordt er geen verdere invulling gegeven wat deze maatregelen minimaal moeten bevatten (zoals dat wel het geval is in de NIS2-richtlijn in artikel 21, lid 2. In de Cbw is Ketenverantwoordelijkheid c.q. Toeleveringsketenbeveiliging niet opgenomen. Wel wordt in Artikel 23, lid 4 een voorzorg gemaakt, omdat hier ook weer te verwijzen naar "Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de in het eerste lid bedoelde maatregelen, waarbij onderscheid kan worden gemaakt tussen sectoren, subsectoren en type entiteiten.". Dus wat niet is kan nog komen.
Artikel 26.1	In de NIS2-tekst staan twee belangrijke dingen: (1) dat maatregelen moeten zijn goedgekeurd door bestuur; en (2) dat bestuur aansprakelijk is voor inbreuken. Echter, de Cyberbeveiligingswet bevat geen bepaling over aansprakelijkheid.
Artikel 27	In de NIS2-richtlijn (RICHTLIJN (EU) 2022/2555 VAN HET EUROPEES PARLEMENT EN DE RAAD van 14 december 2022) wordt in artikel 13, lid 2, gesteld "De lidstaten zorgen ervoor dat hun CSIRT's of, in voorkomend geval, hun bevoegde autoriteiten, meldingen ontvangen van significante incidenten op grond van artikel 23, en van incidenten, cyberdreigingen en bijna-incidenten op grond van artikel 30." In het voorstel van wet (Cyberbeveiligingswet) Artikel 27 staat echter "1. De essentiële entiteit of de belangrijke entiteit meldt overeenkomstig de artikelen 28 tot en met 31 ieder significant

	incident.". Er is dus geen meldingsplicht opgenomen op grond van artikel 30, incidenten (niet significant?), cyberdreigingen en bijna-incidenten(, in Artikel 34 wordt wel gesproken over vrijwillige melding). Echter in het voorstel van wet (Cyberbeveiligingswet) Artikel 32, lid 2, wordt aangegeven "De essentiële entiteit respectievelijk de belangrijke entiteit deelt de ontvangers van haar diensten, die mogelijkerwijs door een significante cyberdreiging in relatie tot het ontvangen van die diensten worden getroffen, onverwijld mee welke maatregelen die ontvangers kunnen nemen in reactie op die dreiging. Indien nodig stelt de entiteit die ontvangers ook in kennis van de desbetreffende significante cyberdreiging. Bovenstaande roept verwarring op. Wordt in artikel 32, lid 2, in plaats van (-)dreiging, (-)incident bedoeld? De meldplicht geldt voor ieder significante incidenten. Een incident is significant volgens de definitie in artikel 27, lid 2 in het voorstel van wet (Cyberbeveiligingswet): Een incident wordt als significant beschouwd als het: • een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken; • andere natuurlijke of rechtspersoon heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Deze omschrijving geeft ruimte tot interpretatie en maakt niet duidelijk wat de wetgever bedoeld en verwacht. In artikel 37 wordt wel aangegeven dat er bij of krachtens algemene maatregel van bestuur nadere regels kunnen worden opgesteld om te bepalen of er sprake is van een significant incident. Tot dan kun je alles eigenlijk beoordelen als niet significant (niet ernstig of niet aanzienlijk) en dus niet meldplichtig.
Artikel 45 lid 1b	Artikel 45 lid 1b kan afhankelijk van de uitwerking voor de leden van DCC dan wel hun klanten praktisch lastig uitvoerbaar zijn. Ik ben er niet direct tegen (het maakt het gebruik van clouds met kans op wisselende IP-adressen lastiger), maar denk ik wel iets om even binnen de werkgroep bij stil te staan. Zeker als het per los IP moet worden doorgegeven kan het bewerkelijk worden (mede omdat elke mutatie binnen 2 weken gemeld moet worden). Voor dit overzicht hebben we overigens al een plek waar het vanuit leveranciers wordt bijgehouden, dat noemen we CIOT.
Artikelen 48 en 45	Artikel 48 zelfde als artikel 45, enkel met een andere termijn/organisatie.

	Oproep mbt artikel 45 en artikel 48 dat de overheid kijkt in hoeverre ze kunnen faciliteren dat dit slechts bij 1 loket/formulier gemeld hoeft te worden die het dan (voor zover nodig) naar beiden doorstuurt (en indien het een papieren formulier betreft te kijken naar de mogelijkheid hetzelfde formulier te gebruiken).
Artikel 50	Artikel 50 kent een plicht om gegevens van domeinnaamhouders te verifiëren (ten minste naam, e-mailadres en telefoonnummer). Dit kan door registrars of registries gedaan worden. In het laatste geval krijg je een uitdaging in de communicatie naar klanten verwacht ik (het is nu soms al lastig).
Ketenverantwoordelijkheid	In de aanloop naar de vertaling van de NIS2-richtlijn in Nederlandse wetgeving is er gesproken over Ketenverantwoordelijkheid c.q. Toeleveringsketenbeveiliging, welke essentiële en belangrijke entiteiten “verantwoordelijkheid” zou geven over de informatiebeveiliging van hun toeleveranciers. Dit was gebaseerd op Artikel 21, lid 2 d) van de NIS2-richtlijn (RICHTLIJN (EU) 2022/2555 VAN HET EUROPEES PARLEMENT EN DE RAAD van 14 december 2022) “d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;”
Certificering	In artikel 24 NIS2-Richtlijn is een mogelijkheid opgenomen voor voorschrijven certificeringen. Lidstaat Nederland heeft er voor gekozen deze bepaling NIET te implementeren. Zij zegt daarover: “Van de mogelijkheid is (nog) geen gebruik gemaakt”. DCC verzoekt u wel voor te schrijven dat ICT-dienstverleners conform de gangbare de ISO 27001 een rechtsvermoeden voor NIS2-compliance oplevert.
Meldplicht	Meldplicht kan exposure geven over een bedrijf. Verzoek om in te regelen dat dit discreet behandeld wordt.