DUTCH DATACENTER ASSOCIATION

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

Betreft: **Internetconsultatie implementatie NIS2-Richtlijn**

Amsterdam, 1 juli 2024

Excellentie,

Hierbij geeft De Dutch Data Center Association (DDA) een reactie op de Internetconsultatie inzake oftewel Implementatiewet tot uitvoering van de Richtlijn (EU) 2022/25551 (hierna: Cyberbeveiligingswet).

Als datacenter sector staan we voor een veilige en weerbare digitale infrastructuur en zijn verheugd dat vernieuwde regelgeving geïmplementeerd gaat worden die de cyberveiligheid van Nederland gaat vergroten.

Voor deze reactie heeft DDA de Cyberbeveiligingswet, inclusief de Memorie van toelichting (hierna MvT), alsmede de NIS2 Richtlijn (EU) 2022/2555 (hierna: NIS2-Richtlijn) gebruikt.

Algemene punten:

- De NIS2-richtlijn heeft voor nu nog onvoldoende verbinding met de dagelijkse praktijk. Er is onvoldoende aandacht voor problematiek van schaarse mankracht en deskundigheid (zowel kennis als ervaring). Van de GDPR hebben we geleerd dat regelgeving vooraf beter op effectiviteit en uitvoerbaarheid getoetst moet worden. Tevens is het voorstel niet afgestemd met andere ambities zoals het versterken en groeien van de eigen digitale infrastructuur spelers.
- Er is te weinig oog voor bestaande oplossingen die reeds werken, zoals bestaande richtlijnen en internationale certificeringen die voor meer effectiviteit zorgen. Een specifieke aanpak van juist de probleemgebieden mist in het voorstel. Men valt terug in te hoog over regulering die juist het einddoel, cyberveiligheid, niet altijd doen verbeteren.
- Als sector willen we vragen voor overzicht en duidelijkheid betreft de meldplicht. En omwille van de regeldruk, is het belangrijk dat dubbele meldplicht zoveel mogelijk beperkt wordt. Dit zou mogelijk zijn door de meldplichten zoveel mogelijk met elkaar in lijn te brengen en het aantal loketten (NCTV, NCSC, CSIRT-DSP, RDI, AIVD, Enisa, enz.) te concentreren.

Specifiek rond datacenters:

- De huidige versie van de Cyberbeveiligingswet roept onduidelijkheden op rond de definitie van een datacenter en de diensten die een datacenter levert. Vele datacenters in Nederland verhuren faciliteiten als ruimte, koeling en stroom aan klanten. Deze klanten plaatsen hun servers in de gebouwen die worden beheerd door de datacenter operator. Deze datacenter eigenaren hebben dus geen zeggenschap over de ICT in het datacenter. Het is onduidelijk waar datacenters als facilitaire partij aan moeten voldoen aangaande cyber beveiliging volgens deze richtlijn. Wat wordt verstaan onder incidenten? Waar over moet worden gerapporteerd? En welke diensten worden bedoeld? Ook de huidige parallel lopende Europese uitwerking die nu in consultatie is, de ‘Cybersecurity risk management & reporting obligations for digital infrastructure, providers and ICT service managers’ /Comite C127400, pagina 11 /artikel 8, biedt geen duidelijkheid voor datacenters en lijdt daardoor niet tot praktisch werkbaar beleid. In de introductie worden de technische en methodologische vereisten (Par 1/pagina 1) besproken, deze vereisten zouden veel duidelijker moeten voor

datacenter diensten. De incident definities voor andere sectoren treden daarentegen veel meer in detail. Wij zouden dit ook graag zien voor de datacenter sector.
- Daarbij leggen de regels ook een grote administratieve last bij de datacenters. Met name het beheren van de risico's van derden. Deze informatie opvragen bij leveranciers en vervolgens zelf deze informatie ook moeten leveren aan klanten zal veel extra administratief werk opleveren.

In detail:
In het wetvoorstel en de MvT worden de termen 'kritieke entiteiten', 'essentiële entiteiten' en 'vitale infrastructuur' gebruikt. Wordt hiermee hetzelfde bedoeld? Bijvoorbeeld, in de MvT 'kritieke entiteiten' wordt genoemd refererend aan art. 2 van de NIS2 Directive. Verduidelijkende vraag: Is dit hetzelfde als de vermelding van 'essentiële entiteiten' genoemd in de Cyberbeveiligingswet?

Blz 5 - 8
Waarom worden datacentra hier niet in genoemd en wel in andere lijsten? Dit is niet logisch en schept onduidelijkheid.

Blz 17 48 Lid 1
Dit is onduidelijk. Moet er informatie worden verstrekt direct aan een EU-entiteit en niet aan een centrale NL-meldpunt? Zo ja, welk meldpunt?

Blz 25 - 70,71 (+ art 80)
Hoe komen de audit criteria tot stand? Wordt er gebruik gemaakt van normenkaders, zoals ISO 27001 of ISAE 3000?

Blz 26 - 76a
Waarom zijn deze artikelen niet van toepassing op overheidsinstanties?

Blz 23 - 5.3
Wat is ertegen om regulier ISO 27001 of NEN 7510 certificaties te accepteren als bewijs van het voldoen aan de Cbw (mits in de VvT de genoemde maatregelen als toegepast aangemerkt staan). Dit zou duidelijkheid scheppen en praktische handvatten bieden voor de entiteiten, wat de minimumeisen zijn om te voldoen aan de wet en de opvolging hieraan.

MvT
We zouden graag zien dat er wordt ingezet op harmonisatie, de volgende opmerking in de MvT baart ons zorgen: "In de amvb wordt naar verwachting gebruik gemaakt van deze ruimte uit de richtlijn om maatregelen vast te stellen die een hoger cyberbeveiligingsniveau waarborgen." Deze opmerking doet blijken dat Nederlandse partijen aan andere/hogere eisen moeten voldoen dan andere partijen, dit lijkt ons onswenselijk.

Tot slot
DDA hoopt dat u onze aandachtspunten en adviezen mee wilt nemen in uw verdere uitwerking van de Cyberbeveiligingswet. Wij zijn natuurlijk bereid onze reactie nadere toelichting te geven.

Hoogachtend,

Stijn Grove
Managing Director
Dutch Data Center Association
www.dutchdatacenters.nl