DUTCH
DATA CENTER
ASSOCIATION

Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

Amsterdam, 28 maart

Onderwerp: Reactie internetconsultatie Cyberbeveiligingsbesluit (Cbb)

Geachte heer/mevrouw,

De Dutch Data Center Association (DDA), de brancheverenigingvoor datacenters in Nederland, verwelkomt de mogelijkheid om te reageren op het Cyberbeveiligingsbesluit. Als fundament van de digitale economie spelen datacenters een cruciale rol in de nationale cybersecurity. Daarom erkennen wij het belang van een hoogwaardige cyberbeveiliging en verwelkomen wij de herziening van de regelgeving om de digitale weerbaarheid van Nederland te versterken. Wel willen wij benadrukken dat het van belang is dat deze regelgeving proportioneel en uitvoerbaar is. In onze reactie lichten wij toe welke aandachtspunten essentieel zijn voor een effectieve en werkbare implementatie van het besluit binnen de datacentersector.

We hebben de consultatiedocumenten met betrekking tot het Cyberbeveiligingsbesluit (Cbb) en de bijbehorende Nota van Toelichting (NvT) zorgvuldig bestudeerd.

Algemene opmerkingen

- **Toepassingsbereik en Duidelijkheid:** We dringen aan op een heldere definitie van het toepassingsbereik van het Cbb, met name in relatie tot datacenters. Hoewel datacenters specifiek genoemd worden in de Uitvoeringsverordening (EU) 2024/2690, is het cruciaal dat de Nederlandse implementatie geen onnodige overlap of tegenstrijdigheden creëert. Duidelijkheid is essentieel om te zorgen voor een consistente en effectieve implementatie.
- **Risicogebaseerde Benadering:** We ondersteunen de risicogebaseerde benadering die in het Cbb wordt gehanteerd. Het is van belang dat de maatregelen die datacenters moeten nemen, evenredig zijn aan de risico's die zij lopen en de impact die een eventueel incident kan hebben. Deze benadering moet ook worden doorgetrokken in het toezicht en de handhaving.
- **Harmonisatie met Bestaande Standaarden:** We pleiten voor maximale harmonisatie met bestaande standaarden en certificeringen (zoals ISO 27001). Dit voorkomt onnodige administratieve lasten en zorgt ervoor dat datacenters kunnen voortbouwen op de investeringen die ze al hebben gedaan in cyberbeveiliging.
- **Regeldruk:** De datacentersector erkent de noodzaak van versterkte cyberbeveiliging, maar maakt zich zorgen over de toenemende regeldruk. Uit onderzoek blijkt dat bedrijven in de sector al aanzienlijke maatregelen hebben genomen op basis van bestaande wetgeving, zoals de Wbni, AVG en sectorspecifieke regels, en sector standaarden, reeds bestaande certificeringen en internationale regelgeving. Zoals beschreven in de NvT leidt het Cbb naar

verwachting tot zowel eenmalige als structurele extra kosten. Hoewel de sector het belang van maatregelen voor netwerk- en informatieveiligheid erkent, is het cruciaal dat deze haalbaar en betaalbaar zijn, met name voor het mkb. Duidelijkheid over het toepassingsbereik, de proportionaliteit van eisen en ondersteuning vanuit de overheid (o.a. handreikingen) zijn essentieel.

Daarnaast is er bezorgdheid over de cumulatieve regeldruk. Er loopt momenteel een onderzoek door de ATR naar de regeldruk in de datacentersector, en de sector vreest dat het Cbb deze druk verder zal verhogen. We pleiten daarom voor een zorgvuldige (internationale) afweging van de noodzaak en effectiviteit van de nieuwe maatregelen, om te voorkomen dat de regeldruk onevenredig wordt, uit de pas loopt met andere Europese landen en de innovatie en groei van de sector belemmert.

Artikelsgewijze punten

- **Artikel 18:** In artikel meent het Cbb dat de entiteit periodiek de doeltreffendheid van de maatregelen moet evalueren. Het is echter onduidelijk wat met periodiek wordt bedoeld, eens per jaar, eens per twee jaar? Daarnaast is het ook onduidelijk wat het evaluatiekader is waarop geconcludeerd kan worden dat maatregelen doeltreffend zijn.
- **Artikel 21:** De Cbb eist dat bestuurders een externe training ondergaan. Door de breed geadopteerde standaarden, zoals ISO 27001, hebben veel bestuurders in onze sector al de benodigde kennis. Daarom zien wij het als een onnodige kostenpost, wanneer dit dan ook nog extern ingekocht moet worden.
- **Artikel 22:** Ook is het onduidelijk wat wordt bedoelt met “onafhankelijk”. Een organisatie zou zelf ook in staat kunnen zijn om een onafhankelijke training/trainer aan te bieden. Daarnaast is het onduidelijk hoe wordt aangetoond dat een trainer “gekwalificeerd” is. Zijn voor deze trainers ook al standaarden of certificeringen vastgesteld? En als bedrijven zelf deze kennis al in huis hebben, waarom zouden ze dan een trainer aanstellen?

Aanbevelingen

- **Ondersteuning en Handreikingen:** We pleiten voor de ontwikkeling van sector specifieke handreikingen, tools en sjablonen om datacenters te ondersteunen bij de implementatie van het Cbb. Dit is vooral belangrijk voor het mkb in de sector.
- **Ingroeiperiode:** We vragen om een redelijke ingroeiperiode na de inwerkingtreding van het Cbb. Dit stelt datacenters in staat om de nodige aanpassingen door te voeren en te voldoen aan de nieuwe eisen.
- **Dialoog:** We pleiten voor een voortdurende dialoog tussen de overheid en de datacentersector om de implementatie van het Cbb te optimaliseren en knelpunten tijdig te adresseren.

Conclusie

De datacentersector is bereid om een constructieve bijdrage te leveren aan de implementatie van het Cbb. We zijn van mening dat een heldere, risicogebaseerde en

geharmoniseerde aanpak essentieel is om de cyberbeveiliging in Nederland effectief te versterken en de continuïteit van digitale diensten te waarborgen.

Met vriendelijke groet,

Stijn Grove
Managing Director, Dutch Data Center Association

Contactgegevens:
Dutch Data Center Association
T - 020 303 7860
E - info@dutchdatacenters.nl
W - www.dutchdatacenters.nl