Notitie NIS2 en Cbw internetconsultatie

Aan: Overheid.nl | Consultatie Cyberbeveiligingswet (internetconsultatie.nl)
Van: Contact | securityadviesgroep.nl
Onderwerp: Notitie NIS2 en Cbw internetconsultatie
Datum: 27-6-2024
cc: --

Inleiding

Internetconsultatie Cyberbeveiligingswet (Cbw)

Onlangs een internetconsultatie gestart rond de Cyberbeveiligingswet (Cbw). Dit wetsvoorstel implementeert de Europese NIS2-richtlijn. 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. Dit doel wordt in Nederland bereikt door, ter implementatie van deze richtlijn, in dit wetsvoorstel onder meer verplichtingen op te leggen aan die entiteiten, zoals het treffen van adequate beveiligingsmaatregelen en het melden van ICT-incidenten.

Reactie Security Adviesgroep als onafhankelijk partner in beveiliging en veiligheid

Als veelzijdig en onafhankelijk partner adviseert en ondersteunt Security Adviesgroep uiteenlopende organisaties in de zorg- en meldplicht ten aanzien van beveiliging en veiligheid. Een multidisciplinair team van beveiligingsprofessionals en juristen hebben de uitnodiging aangenomen om inhoudelijk te reageren op het wetsvoorstel dat via benoemde internetconsultatie is voorgelegd.

Inhoudelijke feedback op internetconsultatie Cbw

Governance NIS2-richtlijn ontbreekt in wetsvoorstel

In artikel 26 van de Cbw is een vrij heldere bepaling opgenomen voor de governance van de cyberbeveiliging binnen essentiële en belangrijke entiteiten. In tegenstelling tot de NIS2-richtlijn ontbreekt in het voorstel de wijze waarop Nederland zorgdraagt voor de aanmoediging om regelmatig een soortgelijke opleiding aan werknemers van essentiële en belangrijke entiteiten aan te beide, zodat zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerpraktijken op het gebied van cyberbeveiliging en de gevolgen ervan voor die diensten die door de entiteit worden verleend te kunnen beoordelen. Zie artikel 20 lid 2 van de NIS2.

Uitwerking zorgplicht

Artikel 23 leden 1,2 en 3 van het voorstel Wwke werken de zorgplicht uit zoals bedoeld in artikel 21 van de NIS2-richtlijn. De uitwerking is in het wetsvoorstel beperkt tot de zorgplicht zelf, zonder een opsomming van de onderwerpen die die maatregelen minimaal moeten bevatten, zoals vermeld in artikel 21 lid 2 van de NIS2-richtlijn. In de memorie van toelichting worden de minimale onderdelen weliswaar vermeld, maar voor de duidelijkheid en de volledigheid van wet, is het logisch om in ieder geval ook in de wet de opsomming van deze onderdelen vanuit de NIS2-richtlijn op te nemen.

Sector overschrijdende aanpak

Artikel 23 lid 4 van het voorstel Cbw bepaalt dat er bij AMvB regels worden gesteld over de maatregelen, waarbij er onderscheid kan worden gemaakt tussen sectoren en subsectoren. Wij kunnen ons vinden in een sectorgewijze uitwerking. Wij vragen ons wel af hoe voorkomen wordt dat er grote verschillen gaan ontstaan tussen deze sectoren die ongewenst zijn. Mogelijk kan in de Cbw een aanwijzingsbevoegdheid voor de Minister van Justitie en Veiligheid worden opgenomen waar sectorale bevoegde autoriteiten zich hebben te voegen.

Rubricering van informatie

Bij de opsomming van mogelijke maatregelen zoals vermeld in artikel 21 lid 2 sub d) van de NIS2-richtlijn wordt melding gemaakt van de beveiliging van de toeleveringsketen. Wanneer essentiële entiteiten en belangrijke entiteiten overwegen welke maatregelen in dit verband passend zijn, moeten zij rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures. Deze verplichting is niet uitgewerkt in de wet zelf, maar hier wordt naar verwezen in de memorie van toelichting van de wet. Overigens zonder verdere toelichting vanuit de wetgever.
Voor essentiële entiteiten en belangrijke entiteiten die onder de aanbestedingsregelgeving vallen kan het van belang zijn dat er specifieke wet-of regelgeving komt waarin een goede rubricering van vertrouwelijke informatie geregeld wordt. Veel organisaties komen niet toe aan het rubriceren van hun (niet digitale) informatie. De rubricering van informatie zou meer aandacht moeten verdienen, zodat ook in het verwervingsproces in de toeleveringsketen beter rekening kan worden gehouden met veiligheidsaspecten. Hierdoor kunnen essentiële entiteiten en belangrijke entiteiten ook in het verwervingsproces de veiligheid effectiever borgen. Wij stellen voor rubricering van informatie expliciet op te nemen als maatregel in het kader van de Cbw wat per sector uitgewerkt kan worden in een AMvB.

Bestuursdwang of zelf monitoren, evalueren en aanpassen van maatregelen

Artikel 21 lid 4 van de NIS2-richtlijn is niet verwerkt in het voorstel Cbw. In de transponeringstabel in de memorie van toelichting is weliswaar aangegeven dat deze bepaling uitgewerkt zou zijn in de artikelen 72 en 73 van het wetsvoorstel, dit kunnen wij echter niet daarin lezen. De artikelen 72 en 73 van het voorstel Cbw gaan over een aanwijzing of last onder bestuursdwang vanwege de bevoegde autoriteit. Oftewel een regeling voor het geval de bevoegde autoriteit heeft vastgesteld dat een entiteit niet voldoet aan de bedoelde maatregelen in lid 2 van artikel 21 van de NIS2-richtlijn. Artikel 21 lid 4 van de NIS2-richtlijn regelt echter de situatie dat een entiteit zelf vaststelt dat deze niet voldoet aan de bedoelde maatregelen. Ons inziens houdt dit in dat er een mechanisme moet komen dat er voor zorgt dat entiteiten zelf de genomen maatregelen monitoren, evalueren en aanpassen of nieuwe maatregelen nemen als blijkt dat maatregelen niet tegemoet komen aan de zorgplicht. Dit dus los van een mogelijke aanwijzing of last onder bestuursdwang. De wetgever moet hiervoor een regeling treffen. Mogelijk dat het onderdeel kan zijn van de governance, een verplichte jaarlijkse audit waarvan verslag moet worden gedaan in de jaarverslagen, of onderdeel van de voorwaarden van eventueel toepasselijke vergunningen.

Tot slot

In het belang van publieke en private opdrachtgevers, waarvan de meesten worden aangewezen als belangrijke, essentiële of kritieke entiteit, houdt Security Adviesgroep zich aanbevolen om ontwikkelingen rond de Cbw en aanpalende AMvB's te (blijven) spiegelen.