Advies Wetsvoorstel Cyberbeveiligingswet

Op basis van het wetsvoorstel, de staat van cybersecuritymaatregelenimplementatie in Nederland en de doelen die Europe probeert de bereiken met de EU NIS2 Directive adviseer ik het Ministerie van Justitie en Veiligheid aan om het wetsvoorstel te verbeteren.

Constaterende dat:

- de Europese Commissie EU NIS2 (2022/2555) heeft gepubliceerd op 14 December 2022;
- de EU NIS2 nieuwe maatregelen voor aanbieders van essentiële diensten expliciet benoemt (zie artikel 21b);
- landen wordt geacht NIS2 te hebben geimplementeerd per oktober 2024;
- het wetsvoorstel gepubliceerd op 21 mei 2024 geen nieuwe maatregelen voorschrijft aan aanbieders van essentiele diensten die de onderwerpen van de EU nis2 benoemt.

Overwegende dat:

- aanbieders van essentiële diensten sinds invoering van de WBNI (9 november 2019) t.b.v. EU NIS Directive (2016/1148) risicomanagementmaatregelen geïmplementeerd moet hebben;
- de NIS2 explicitiet managementverantwoordelijkheid benoemt;
- het doel van de NIS2 is om de cybersecurity van Europa te harmoniseren;
- het aantal (succesvolle) cyberaanvallen toeneemt zoals beschreven in het rapport van de EU agentschap voor cybersecurity ENISA (ENISA Threat Landscape 2023);
- omringende landen, overheden (Duitsland middels BSI-Gesetz, Belgie middels NIS2-wet) wel cybersecuritymaatregelen opdragen aan aanbieders van essentiële diensten;
- het beveiligen van kritieke infrastructuur meerjarige investeringen behelst;
- cybercriminelen en Advanced Persistent Threats (APT's) niet wachten op de implementatie van cybermaatregelen door aanbieders van essentiele diensten;
- de Baseline Informatiebeveiliging Overheid en de Cybersecurity Implementatierichtlijn Objecten Rijkswaterstaat van toepassing is voor onvoldoende sectoren en industrieën vergeleken met de NIS2 en de EU CER (2022/2557), en niet van toepassing is voor private ondernemingen.

Draagt op:

- de cybersecurity maatregelen zoals in artikel 21.2 benoemt zijn toe te voegen:

"De in lid 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende:

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b) incidentenbehandeling;
c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;
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;

e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit."

- de toezichthouder een update te doen aan de BIO en CSIR op basis van internationale standaarden zoals (ISO27002 voor IT en IEC62443 voor Operationele Technology (OT)) en die verplicht te stellen (middels comply-or-mitigate model) aan aanbieders van essentiële diensten;
- managementverantwoordelijkheid niet te vertragen met 2 jaar, en te maximeren op 6 maanden na installatie;
- aanbieders van essentiële diensten een jaarlijkse audit o.b.v. de NIS2 maatregelen uit laat voeren door de toezichthouder, geaccrediteerde certificatie-instelling of gecertificeerde informatiebeveiligings-/cybersecurityauditors.