Datum: 1 juli 2024
Betreft: Consultatiereactie Cyberbeveiligingswet

De chemie van verbinden

Introductie

Het VHCP is de brancheverenigingvoor de chemieketen. Onder onze leden bevinden zich chemiedistributeurs, opslagbedrijven, transportbedrijven en verpakkingsbedrijven.

Met deze activiteiten, die allemaal betrekking hebben op de chemische sector, zijn onze leden aangewezen als 'belangrijke entiteit' onder de Cyberbeveiligingswet. Deze wet strekt tot implementatie van de Europese richtlijn Network and Information Security (NIS2).

Aandachtspunt 1: Bied duidelijkheid aan bedrijven gevestigd in meerdere lidstaten

Zoals volgt uit artikel 23 van de NIS2-richtlijn is er een registratie-, zorg- en meldplicht voor essentiële en belangrijke entiteiten. Zij moeten elk significant incident melden bij hun Computer Security Incident Response Team (CSIRT) en de toezichthoudende instantie. Duidelijk is ook dat de CSIRT's uit verschillende lidstaten met elkaar samenwerken om snel te communiceren over grensoverschrijdende cyberincidenten.

Uit de voorgestelde Cyberbeveiligingswet komt echter nog niet helder naar voren hoe de wet omgaat met bedrijven die gevestigd zijn in meerdere landen. VHCP-leden zouden graag antwoord zien op de volgende vraag:

- Een bedrijf is in lidstaat A en B gevestigd;
- De veiligheidsverantwoordelijke van het bedrijf opereert namens het bedrijf in lidstaat A, maar de cyberbeveiliging wordt in lidstaat B geregeld;
- Er is een bedreiging voor de cyberveiligheid in lidstaat B;
- Kan de veiligheidsverantwoordelijke dan in zijn eigen lidstaat A melden, of moet dit via lidstaat B omdat daar een veiligheidsincident plaatsvindt?
- Dezelfde vraag geldt wanneer de veiligheidsverantwoordelijke in lidstaat B opereert, in lidstaat B ook de cyberveiligheid wordt geregeld, en het incident in lidstaat A plaatsvindt.

Met andere woorden: het VHCP zou graag opheldering willen over de samenhang tussen verschillende lidstaten en waar de primaire meldplicht ligt als de cyberveiligheid grensoverschrijdend is geregeld.

Aandachtspunt 2: Voorkom verwarring over toezichthoudende instanties

Zoals uiteengezet in paragraaf 5.7.13 in de MvT bij het wetsvoorstel, wordt het toezicht op de verplichtingen vormgegeven langs de lijnen van de ministeriële verantwoordelijkheden voor de respectievelijke gereguleerde sectoren. Voor de chemiesector zijn meerdere toezichthoudende instanties actief, waarvan onder andere de Inspectie Leefomgeving & Transport (ILT) en de Omgevingsdiensten (OD's). Bij incidenten met betrekking tot veiligheid en milieu kan in sommige gevallen bij beide instanties melding worden gedaan. Een deel van onze leden is daarnaast gereguleerd onder de Europese Seveso-richtlijn.[1] De toezichthoudende instanties voor de Seveso-bedrijven, veelal OD's, hebben aangekondigd het aspect cyberweerbaarheid mee te nemen in hun inspecties.

In het geval van de voorgestelde Cyberbeveiligingswet leiden de lijnen van ministeriële verantwoordelijkheden voor de chemiesector er naar verwachting toe dat de ILT toezicht zal houden

[1] In Nederland geïmplementeerd via de Omgevingswet en het Besluit activiteiten Leefomgeving.

op naleving.[2] Dat betekent dat bij een incident dan ook melding moet worden gemaakt bij de ILT. Om te voorkomen dat verwarring ontstaat moet dit gegeven duidelijk aan bedrijven gecommuniceerd worden. Daarnaast moet duidelijk zijn welke verplichtingen leidend zijn als het gaat om cyberveiligheid bij Seveso-bedrijven. Het VHCP ziet ernaar uit dat dit duidelijk wordt aangegeven in de MvT van de voorgestelde wet en in de afgeleide lagere regelgeving, en roept op tot heldere communicatie richting de gereguleerde bedrijven over hun verplichtingen.

Aandachtspunt 3: Aantonen van compliance met NIS2

Omdat aangesproken entiteiten niet alleen hun eigen cybersecurity op orde moeten hebben, maar ook rekening moeten houden met de specifieke kwetsbaarheden van hun rechtstreekse leveranciers en dienstverleners, signaleert het VHCP dat veel bedrijven direct of indirect via deze ketenverantwoordelijkheid zullen worden aangesproken op de eisen uit de NIS2-richtlijn. Daarom doet het VHCP de suggestie aan het ministerie van Justitie en Veiligheid om na te denken over een manier voor bedrijven om compliance met de NIS2-eisen aan te tonen. Dit is specifiek relevant voor bedrijven die zelf niet onder de Cyberbeveiligingswet vallen maar dienstverlener zijn aan een bedrijf die wel onder de wet valt. Het zou bedrijven helpen om dan met bijvoorbeeld een certificaat aan te kunnen tonen dat zij hun cyberbeveiliging conform NIS2 op orde hebben. Een dergelijke aanpak zou de regeldruk bij bedrijven kunnen wegnemen en het bewustzijn van het belang van cybersecurity in den brede doen verhogen.

[2] Zie de aankondiging van de ILT op de website: Toezicht op cybersecurity | Inspectie Leefomgeving en Transport (ILT) (ilent.nl).