Ministerie van Justitie & Veiligheid
Directie Wetgeving en Juridische Zaken
Postbus 20301
2500 EH DEN HAAG

centraal bureau levensmiddelenhandel

Bezoekadres
Overgoo 13
2266 JZ Leidschendam

Postadres
Postbus 262
2260 AG Leidschendam

070 - 337 62 00
info@cbl.nl

Datum 25 juni 2024

Betreft Reactie CBL internetconsultatie Cyberbeveiligingswet

Via deze weg reageert het Centraal Bureau Levensmiddelenhandel (CBL) graag op de internetconsultatie over de Cyberbeveiligingswet, die dient als implementatie van de Europese NIS2-richtlijn. Het CBL is de brancheverteegenwoordiger van supermarkten en foodservicebedrijven. Het CBL herkent de noodzaak voor aandacht met betrekking tot cyberbeveiliging en deelt een aantal aandachtspunten voor de verdere voorbereiding van het wetsvoorstel.

Uniformiteit, consistentie en proportionaliteit

Het CBL benadrukt de noodzaak om te streven naar uniformiteit, consistentie en proportionaliteit in de implementatie van de NIS2-richtlijn. Zo is het van groot belang dat de reikwijdte en definities van verschillende Europese regelingen zoveel mogelijk op elkaar aansluiten, waardoor organisaties hun processen beter kunnen stroomlijnen en zich kunnen richten op efficiënte naleving. Daarnaast is het essentieel om nationale, regionale en lokale verschillen in regelgeving zoveel mogelijk te vermijden door de NIS2-richtlijn beleidsarm in te voeren. Bij keuzes in de implementatie van de richtlijn moet rekening worden gehouden met de lastendruk voor bedrijven.

Verder moeten de standaarden werkbaar en proportioneel zijn, en de nalevingskosten, administratieve lasten en toezichtslasten zoveel mogelijk worden beperkt. Dit is met name van belang voor ondernemers in de levensmiddelensector, die al snel onder de NIS2 vallen. Gestandaardiseerde en eenduidige hulpmiddelen en regelingen, met een centraal loket voor ondernemers en goede ICT-tools, zijn noodzakelijk voor een soepele implementatie.

De negatieve gevolgen van een doorsijpeleffect naar het MKB moeten zoveel mogelijk worden beperkt. Dit betekent dat het effect van regelgeving op MKB-bedrijven, die strikt genomen buiten de reikwijdte vallen, goed in kaart moet worden gebracht middels een MKB-toets en gemitigeerd. Tot slot zijn evaluatiemomenten essentieel om te voorkomen dat regels overbodig of ineffectief zijn. Hierbij is het belangrijk om samen te werken met de betreffende (sub)sectoren om de regelgeving voortdurend te verbeteren en aan te passen aan de praktijk.

Reikwijdte

Een punt van zorg is de uitbreiding van de reikwijdte in de implementatie van de NIS2-richtlijn, van netwerk- en informatiesystemen die belangrijk zijn voor de essentiële dienstverlening, naar *alle* netwerk- en informatiesystemen die entiteiten voor hun werkzaamheden of diensten gebruiken, inclusief hun fysieke omgeving. Bedrijven zouden hun focus en inspanning moeten richten op de beveiligingsrisico's van netwerk- en informatiesystemen die cruciaal zijn voor de essentiële of belangrijke dienstverlening, met uiteraard aandacht

voor de koppelvlakken. In het verlengde hiervan moet de risicogerichte benadering als rode draad door alle aspecten van de implementatie van wet- en regelgeving lopen.

Een specifieke vraag hierbij betreft de uitwerking van het wetsvoorstel op bedrijven die wel betrekking hebben op één of meer van de sectoren opgenomen in Bijlage 1 en 2 bij het wetsvoorstel, maar waarvoor dit niet de *kerntaak* of -activiteit is. Dit is met name relevant voor de categorieën “Digitale Infrastructuur” en “Beheer van ICT-diensten (business-to-business)”, waaronder een aantal diensten valt die veelal binnen bedrijfsgroepen door één entiteit aan een andere entiteit of franchisenemer worden verstrekt. Denk hierbij aan het gebruik van datacentercapaciteit van één groepsmaatschappij door andere groepsmaatschappijen of franchisenemers, bijvoorbeeld omdat het niet efficiënt is als elke entiteit haar eigen datacentercapaciteit regelt. Valt de groepsmaatschappij die datacentercapaciteit levert in dit geval onder het wetsvoorstel, ongeacht of de dienst aan essentiële of belangrijke dienstverleners wordt geleverd? Of is er – in het geval van bijvoorbeeld beheerde beveiligingsdiensten – geen sprake van “business-to-business” dienstverlening wanneer het dienstverlening binnen dezelfde bedrijfsgroep of concern betreft? Het is belangrijk dat de uitwerking in het uiteindelijke wetsvoorstel uitgaat van de beoogde risicogerichte benadering.

Inwerkingtreding en verhouding met ISO 27001

Het CBL constateert enkele onzekerheden en zorgen met betrekking tot de Cyberbeveiligingswet. Zo is nog onduidelijk wanneer de Cyberbeveiligingswet nu exact in werking treedt en de vereisten voor organisaties tijdens de voorbereidingsfase. Voor een goede uitvoering is het essentieel dat bedrijven ruimschoots voor de inwerkingtreding duidelijkheid hebben over het tijdspad en de te nemen maatregelen. Het recente uitstel van de inwerkingtreding roept vragen op over de reden hiervan en wat in de tussentijd precies van organisaties wordt verwacht.

In algemene zin constateert het CBL dat de NIS2-richtlijn veel raakvlakken vertoont met onder andere ISO 27001 en NIST Cyber Security Framework. Hieruit volgen enkele onduidelijkheden met betrekking tot de onderlinge verhoudingen. Een organisatie kan bijvoorbeeld al voldoen aan de certificering voor ISO 27001, maar het is nog onduidelijk of een organisatie hiermee ook voldoet aan de vereisten uit de NIS2-richtlijn, of dat er nog additionele maatregelen genomen moeten worden. Het toezicht roept eveneens vragen op. Zo is er bij de ISO 27001 sprake van toezicht vooraf waarbij organisaties een certificering krijgen die jaarlijks herzien moet worden. De vraag is of dit consequenties heeft voor het toezicht onder de Cyberbeveiligingswet.

Het CBL zou graag snel duidelijkheid zien over de verwachte kosten voor belangrijke entiteiten. In artikel 17 staat dat belangrijke entiteiten zelf de kosten dragen voor proactief uitgevoerde beveiligingsscans door een CSIRT, verzocht door de belangrijke entiteit. Tegelijkertijd bepaalt artikel 79 dat de kosten voor beveiligingsscans, verzocht door de bevoegde autoriteit, in sommige gevallen (nader uit te werken in een AMvB), bij de belangrijke entiteit komen te liggen. Het is van belang dat er snel duidelijkheid komt over de specifieke gevallen waarin de kosten voor beveiligingsscans verplicht bij de entiteit komen te liggen. Het uitgangspunt moet zijn, conform artikel 79, lid 2, dat deze kosten in principe bij de bevoegde autoriteit liggen.

Toeleveringsketen

Ten aanzien van de beveiliging van de toeleveringsketen heeft het CBL enkele belangrijke aandachtspunten. De NIS2-richtlijn vereist dat essentiële en belangrijke entiteiten rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener (zoals uiteengezet in artikel 21, lid 3 in de NIS2-richtlijn), en de algemene kwaliteit van hun producten en cyberbeveiligingspraktijken. Ook moeten zij rekening houden met de resultaten van gecoördineerde risicobeoordelingen van kritieke toeleveringsketens (zoals uiteengezet in artikel 22 in de NIS2-richtlijn).

Voor supermarkten en foodservicebedrijven is het praktisch onmogelijk om deze mate van toezicht en coördinatie te realiseren, gezien het grote aantal verschillende grote en kleine leveranciers. Het continue bijhouden en coördineren van de specifieke kwetsbaarheden en cyberbeveiligingspraktijken van al deze leveranciers leidt tot een zeer grote stijging van de administratieve lasten en maakt de naleving van de NIS2-richtlijn zeer uitdagend.

Daarnaast constateert het CBL dat er toezicht zal plaatsvinden in de vorm van audits. Bij de huidige praktijk van ISO-certificeringen wordt een leveranciersbeoordeling gedaan om te garanderen dat leveranciers voldoen aan de richtlijnen voor informatiebeveiliging. Het CBL ziet graag duidelijkheid of dit ook op dezelfde manier zal gelden, en zo niet, wat hiervoor de achterliggende reden is. Het CBL concludeert dat de huidige eisen voor leveranciersbeoordeling in de NIS2-richtlijn in de praktijk zeer moeilijk uitvoerbaar zullen blijken voor veel sectoren.

Zorgplicht en significante incidenten

Het CBL wil enkele aandachtspunten naar voren brengen met betrekking tot de zorgplicht en de omgang met significante incidenten. Artikel 23 van de Cyberbeveiligingswet beschrijft de zorgplicht, waarbij het CBL zich afvraagt waarom de maatregelen zoals omschreven in artikel 21 van de NIS2-richtlijn, niet expliciet één-op-één zijn overgenomen. Deze richtlijn geeft immers minimumeisen aan. In de concept-memorie van toelichting worden de minimumeisen uit artikel 21 van de NIS2-richtlijn wel genoemd. Dit leidt tot de assumptie dat de omschreven maatregelen in artikel 21 van de NIS2-richtlijn voldoende zijn voor de naleving, al is het wenselijk dat dit punt op de korte termijn wordt opgehelderd.

Verder is er aandacht voor de openbaarmaking van significante incidenten in artikel 39 van de Cyberbeveiligingswet. Doordat de term ‘kan veroorzaken’ voor meerdere interpretaties vatbaar is, is het nu niet duidelijk genoeg onder welke voorwaarden een significant incident gemeld moet worden. De NIS2-richtlijn definieert dit als een incident met aanzienlijke gevolgen, maar incidenten lijken onder de voorgestelde definitie een bredere reikwijdte te hebben. Dit zouden nu ook operationele (IT) incidenten kunnen omvatten, terwijl de richtlijn tot doel heeft om de cyberbeveiliging te verhogen. Het CBL raadt aan om de meldplicht daarom in lijn te brengen met deze doelstelling.

Het CBL vindt het van belang om dubbele meldingen zoveel mogelijk te voorkomen. Dit kan worden voorkomen door een duidelijkere definitie te hanteren wie een incident moet melden bij welke toezichthouder. Bijvoorbeeld: bij een nationaal significant incident op pinbetalingen zou nu onduidelijk zijn of een winkel of betreffende bank(en) moeten voldoen aan hun meldplicht. Bovendien zijn sommige organisaties in verschillende lidstaten actief. Het CBL zou graag zien dat een centraal loket wordt ingesteld voor organisaties die in twee of meer landen actief zijn waar de NIS2-richtlijn geldt. Idealiter zouden deze organisaties één keer een melding kunnen doen, in plaats van dit zelf te moeten doen in alle landen waar de organisatie actief is.

Met betrekking tot de nadere regels over meldingen van significante incidenten (artikel 37 in het conceptwetsvoorstel) vindt het CBL het logisch dat er onderscheid kan worden gemaakt tussen sectoren en subsectoren. Het CBL ziet graag dat dit onderscheid wordt aangebracht in consultatie met de betreffende (sub)sectoren. Wat betreft de drempelwaarden van een significant incident verzoekt het CBL om rekening te houden met de administratieve lasten door de drempelwaarden zoveel mogelijk te harmoniseren met andere lidstaten. Hiermee kan worden voorkomen dat organisaties eenzelfde incident moeten melden bij verschillende toezichthouders in verschillende lidstaten.

Governance

Het CBL heeft enkele aandachtspunten met betrekking tot de governance-vereisten. Zo stelt artikel 26 in het conceptwetsvoorstel dat ieder lid van het bestuur moet beschikken over kennis en vaardigheden op het gebied van de risico's voor de beveiliging van netwerk- en informatiesystemen, evenals risicobeheersmaatregelen en het beoordelen van de gevolgen van deze risico's en risicobeheersmaatregelen. Het CBL constateert een hoge mate van ambiguïteit in deze definitie. Zo is onduidelijk op welk concreet niveau bestuursleden over deze kennis moeten beschikken.

Daarnaast doet de voorgestelde vertaling van de term "bestuur" geen recht aan de praktische realiteit. De NIS2-richtlijn spreekt van "*members of management bodies*". Een betere vertaling zou dan ook zijn om te spreken over "leidinggevenden" en "managers". Het bestuur draagt weliswaar de eindverantwoordelijkheid, maar kan niet alle taken zelf uitvoeren. Vooral in grotere organisaties zal het bestuur de vereiste kennisaspecten aansturen door bijvoorbeeld een security-afdeling in te stellen die de dagelijkse uitvoering op zich neemt. Het bestuur geeft in zulke gevallen sturing op basis van de resultaten. Het risicomanagement ligt meer bij het lijnmanagement, aangezien zij verantwoordelijk zijn voor de uitvoering van de processen en het gebruik van informatie.

Het bestuur moet verantwoordelijk zijn voor het organiseren, initiëren en toezicht houden op het proces van risicobeheersing. Dit omvat het zorgen dat systemen inzichtelijk zijn, toegewezen zijn aan een eigenaar en dat de zorgtaken duidelijk zijn. Het bestuur hoeft echter niet zelf de benodigde expertise te hebben, maar moet ervoor zorgen dat deze expertise beschikbaar is, bijvoorbeeld via een CIO of CISO. Periodieke overleggen met inhoudelijke experts zijn effectiever dan generieke cursussen, die vaak geen specifieke kennis over de eigen organisatie bieden. Het is onrealistisch om te verwachten dat bestuursleden naast hun huidige taken ook cybersecurityrisico's kunnen identificeren en beoordelen, aangezien dit jarenlange ervaring en opleiding vereist. Korte trainingen kunnen dit niet vervangen en de certificaten van dergelijke trainingen zijn weinig waardevol en leiden vaak tot een papieren werkelijkheid.

Goede governance vereist een juiste verdeling van verantwoordelijkheden. Men kan dit vergelijken met kennis op het gebied van financiën en personeel: een manager hoeft geen expert te zijn om verantwoordelijkheid te dragen voor een budget of medewerkers. Het is daarom essentieel dat het uiteindelijke wetsvoorstel voldoende rekening houdt met deze realiteiten en de rol van lijnmanagement expliciet benoemt en erkent in het risicomanagementproces.

Vertrouwelijke gegevens

In artikel 65 staat dat vertrouwelijke gegevens aan onder andere de Europese Commissie kunnen worden verstrekt. Ondanks de minimumvereisten in het eerste lid blijft onduidelijk om wat voor vertrouwelijke gegevens dit precies gaan, behalve dat de verstrekking beperkt blijft tot noodzakelijke en evenredige gegevens.

Daarnaast wordt uit het artikel nog onvoldoende duidelijk op welke wijze de vertrouwelijkheid van de vertrouwelijke gegevens zoveel mogelijk wordt geborgd. Vanzelfsprekend is het onwenselijk dat gevoelige informatie of bedrijfsgeheimen onverhoopt openbaar worden. In een dergelijk scenario is de betrokken entiteit juist extra kwetsbaar voor eventuele dreigingen. Bovendien gaat het bij vertrouwelijke gegevens soms om commerciële informatie die niet bedoeld is voor andere actoren binnen de sector. Zo kan het CSIRT volgens artikel 65, lid 2 vertrouwelijke gegevens verstrekken aan andere essentiële entiteiten, belangrijke entiteiten en andere relevante partijen. Het CBL vindt het verder positief dat deze vertrouwelijke gegevens in ieder geval niet vallen onder de Wet open overheid als maatregel om de vertrouwelijkheid van de gegevens te waarborgen.