Reactie CBL consultatie Cyberbeveiligingsbesluit

Het Centraal Bureau Levensmiddelenhandel (CBL), de koepelorganisatie van supermarkten en foodservicebedrijven, reageert via deze weg graag op de internetconsultatie van het Cyberbeveiligingsbesluit en de onderliggende ministeriële regeling. Het CBL waardeert een tijdige implementatie van de oorspronkelijke NIS2-richtlijn om cyberveiligheid bij bedrijven in o.a. de levensmiddelenbranche te waarborgen. Tegelijkertijd uit het CBL zorgen over de administratieve lasten voor zowel grotere bedrijven als het mkb; in het bijzonder met betrekking tot de grote hoeveelheid documentatie, de trainingsvereisten en het vermijden van dubbele lasten.

Implementatie en inwerkingtreding

De Nederlandse implementatie van de Europese NIS2-richtlijn, voorzien via de Cyberbeveiligingswet en het onderliggende Cyberbeveiligingsbesluit inclusief de ministeriële regeling, heeft al enige keren vertraging opgelopen. Een aantal andere EU-lidstaten zijn momenteel verder dan Nederland in de implementatie. Voor een gelijk speelveld is het daarom van groot belang dat de implementatie van de NIS2-richtlijn geen verdere vertraging oploopt. Momenteel is voorzien dat de Cyberbeveiligingswet in werking treedt in het derde kwartaal van 2025.

Het CBL hecht er echter aan dat de eerste periode na de officiële inwerkingtreding toezichtsluw verloopt in een overgangsperiode zodat bedrijven voldoende tijd hebben om te voldoen aan de vereisten. Zo hebben bedrijven onder de Cyberbeveiligingswet een registratieplicht en dienen zij zich zelf aan te melden bij het Nationaal Cyber Security Centrum (NCSC). Bovendien vraagt het huidige besluit om een grote hoeveelheid aan beleidsplannen en andere documentatie. Concreet vraagt het CBL om een overgangsperiode waarbij de toezichthouder terughoudend optreedt in de handhaving, aangezien deze al handhavend zou kunnen optreden direct vanaf de inwerkingtreding.

De Cyberbeveiligingswet is van toepassing op levensmiddelenbedrijven die actief zijn in industriële productie, verwerking en groothandel van levensmiddelen. Het maakt niet uit of dit een hoofd- of nevenactiviteit is. Levensmiddelenhandelsbedrijven die zich *uitsluitend* richten op distributie richting consumenten (retail) vallen buiten de rijkwijdte van de Cyberbeveiligingswet.

De huidige communicatie hierover is regelmatig verwarrend, vooral voor (mkb-)supermarkten die enkel aan consumenten leveren. Wanneer zij via overheidswebsites proberen te achterhalen of de wet op hen van toepassing is, ontbreekt vaak deze cruciale nuance in de definitie van de levensmiddelensector. Hoewel het CBL voor de branche reeds dient als informatiecontactpunt, zou het helpen in de implementatie als bedrijven met vragen ook terecht kunnen bij de NCSC of een andere entiteit.

Administratieve lasten

Het CBL maakt zich zorgen over de grote hoeveelheid administratieve lasten die het Cyberbeveiligingsbesluit omhelst. Hoofdstuk 4 van het Cyberbeveiligingsbesluit stelt vast dat bedrijven verschillende beleidsdocumenten moeten opstellen voor de (1) beveiliging van netwerk- en informatiesystemen (artikel 6); (2) risicomanagement (artikel 7); (3) incidentenbehandeling (artikel 8); (4) bedrijfscontinuïteit en crisisbeheer (artikel 9); (5) beveiliging van de toeleveringsketen (artikel 10); (6) het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen (artikel 11); (7) gebruik van cryptografie (artikel 13); (8) toegangsbeleid (artikel 15); en (9) beheer van assets (artikel 16). Deze beleidsplannen moeten daarnaast periodiek geëvalueerd worden, welke tevens schriftelijk dienen te worden vastgelegd. Met name voor het mkb zorgt dit voor een grote administratieve last, zeker als zij vanaf een nulpunt in al deze punten moeten voorzien.

Voor bedrijven van alle groottes zouden deze administratieve lasten een aanzienlijke hoeveelheid tijd en middelen in beslag nemen die ook hadden kunnen worden ingezet voor daadwerkelijke cyberbeveiliging. Met name kleinere

bedrijven en het mkb krijgen te maken met een onevenredige hoeveelheid administratieve lasten voor hun capaciteiten en de daarbij hoge kosten. Daarom pleit het CBL voor een meer risicogerichte benadering waarbij bedrijven meer flexibiliteit krijgen om te voorzien in hun praktische invulling van de doelen zoals gesteld in de zorgplicht. De elementen van de zorgplicht (bijvoorbeeld netwerk- en informatiesystemen, risicomanagement, bedrijfscontinuïteit) zouden ongewijzigd kunnen blijven, maar bedrijven zouden zelf moeten kunnen bepalen hoe ze de veiligheid van de respectievelijke elementen waarborgen. Dit zou aanzienlijk schelen in de administratieve lasten zonder dat dit per definitie gevolgen heeft voor de cyberbeveiliging. Daarbij valt op te merken dat mkb-bedrijven, zijnde frachisenemers, steunen op een bestaand netwerk, waardoor verantwoordelijkheden elders in de keten kunnen liggen.

Specifiek voor kleinere en middelgrote levensmiddelenbedrijven verzoekt het CBL om zoveel mogelijk ondersteuning, bijvoorbeeld vanuit het NCSC, om bedrijven te helpen voldoen aan de zorgplicht. Dat zou bijvoorbeeld kunnen via een handleiding en via een bedrijvenloket. Voorkomen moet worden dat bedrijven door de grote hoeveelheid documentatie niet meer toe komen aan de daadwerkelijke cyberbeveiliging.

Voor bedrijven van alle groottes zou het daarnaast aanzienlijk schelen in de regeldruk als zij gebruik kunnen maken van bestaande veiligheidsnormen, bijvoorbeeld de ISO-normen. Het CBL is ermee bekend dat het gebruik van de ISO-normen niet automatisch betekent dat een bedrijf voldoet aan alle eisen uit de Cyberbeveiligingswet en de zorgplicht uiteengezet in het Cyberbeveiligingsbesluit. Toch wil het CBL ervoor waken dat bedrijven te maken krijgen met dubbele lasten of het ‘wiel opnieuw moeten uitvinden’. Het CBL hoopt er daarom op dat bedrijven actieve ondersteuning kunnen krijgen om ervoor te zorgen dat zij eventueel bestaande maatregelen volgens bestaande normen kunnen inpassen in de nieuwe eisen van de Cyberbeveiligingswet en het Cyberbeveiligingsbesluit.

Het CBL leest in artikel 24 dat de respectievelijke vakminister de drempelwaarden voor de kwalificatie van een significant incident vaststelt bij ministeriële regeling. Het CBL benadrukt dat deze drempelwaarden niet te lichtzinnig moeten worden ingeschat en de drempelwaarden zich moeten toespitsen op de essentiële diensten van een bedrijf. Voor bedrijven met meerdere digitale diensten en/of activiteiten, die niet gerelateerd zijn aan de essentiële dienstverlening, zou het onwenselijk zijn als zij te maken krijgen met een te uitgebreide meldplicht.

Overigens vindt het CBL dat dubbele lasten zoveel mogelijk voorkomen moeten worden voor bedrijven die vallen onder zowel de Cyberbeveiligingswet als de Wet weerbaarheid kritieke entiteiten (Wwke). Indien een bedrijf onder beide wetten valt, moet zij de mogelijkheid hebben om met één risicobeoordeling en één maatregelenpakket aan beide wetten te voldoen. Het CBL ziet daarbij geen noodzaak voor afzonderlijke beleidsplannen en andere documentatie. Een geharmoniseerde benadering zou samen moeten kunnen gaan met de zorgplicht uit beide wetten en zou tijd en middelen besparen voor bedrijven en toezichthouders.

Trainingen

Het Cyberbeveiligingsbesluit gaat ook in op de trainingsvereisten waaraan bedrijven in de Cyberbeveiligingswet aan moeten voldoen. In het Cyberbeveiligingsbesluit is dit voorzien in hoofdstuk 5. Artikel 21 en 22 gaan in op respectievelijk de eisen aan de training en de eisen aan de trainer. In de consultatiereactie op de Cyberbeveiligingswet gaf het CBL aan dat zij het onlogisch vindt dat de trainingsvereisten zich enkel richt op bestuurders en niet op de rollen die het meeste met cyberveiligheid bezig zijn.

Artikel 22 stelt dat de training moet worden verzorgd door een onafhankelijke en gekwalificeerde trainer. Volgens het CBL is de kwaliteit van de training niet per definitie gewaarborgd door een onafhankelijk en gecertificeerd karakter. Bovendien leidt deze eis tot hogere implementatiekosten voor bedrijven. Daarom pleit het CBL voor een doelgestuurde aanpak, waarbij de invulling van de trainingen en de vereisten van de trainer aan bedrijven zelf wordt overgelaten. Dit hoeft niet per definitie te leiden tot een verminderde kwaliteit van de training.

Ketenverantwoordelijkheid

Het CBL leest in artikel 10 de verschillende maatregelen die bedrijven moeten nemen voor de beveiliging van de toeleveringsketen. Concreet moeten bedrijven in een beleidsplan beoordelen hoe veilig hun leveranciers zijn en maatregelen moeten nemen om risico's te verkleinen. Het zou hier uitsluitend gaan over de toeleveringsketen met betrekking tot de beveiliging van de netwerk- en informatiesystemen die de entiteit gebruikt. Het CBL benadrukt dat ook hierbij een risicogerichte benadering mogelijk moet zijn waarbij de beoordeling van deze ketenrelaties correspondeert met de eventuele veiligheidsrisico's.

In hetzelfde artikel staat beschreven dat bedrijven schriftelijke afspraken moeten maken met leveranciers over cyberbeveiligingseisen. In de memorie van toelichting wordt terecht opgemerkt dat bedrijven niet altijd in de positie zijn om hierover te onderhandelen met leveranciers. In dat geval wordt wel gekozen voor een risicogerichte benadering en moet een bedrijf zelf nagaan of de leverancier past binnen het gestelde cyberbeveiligingsniveau. Het CBL ziet hierin een goed voorbeeld van doelsturing en een risicogerichte benadering en vindt dat bedrijven zelf de afweging moeten maken of zij in de positie zijn om dergelijke schriftelijke afspraken te maken met hun leveranciers.

In situaties van afhankelijkheidsposities is het wenselijk dat onderliggende partijen, die verplicht gebruikmaken van specifieke ICT-faciliteiten, kunnen vertrouwen op de invulling van de zorgplicht door de betreffende aanbieders. Zo wordt dubbel werk in de beveiliging van de toeleveringsketen voorkomen.

Daarnaast vraagt het CBL nadrukkelijk aandacht voor mogelijke doorsijpeleffecten richting het mkb. Grote bedrijven die onder de NIS2-richtlijn vallen, kunnen immers verplicht zijn uitsluitend samen te werken met leveranciers die aan deze eisen voldoen. Dit kan negatieve gevolgen hebben voor mkb-bedrijven zonder adequate cyberbeveiliging, die hierdoor opdrachten mislopen en zakelijke schade oplopen.

Vertrouwelijkheid van persoonsgegevens

Het CBL constateert in artikel 30 dat persoonsgegevens, afhankelijk van de situatie, tot 60 maanden na de eerste verwerking of laatste wijziging kunnen worden bewaard. In sommige gevallen loopt deze termijn zelfs op tot 120 maanden. Uit de toelichting blijkt dat kortere bewaartermijnen in de praktijk niet haalbaar zijn gebleken. Gezien de langdurige opslag hecht het CBL groot belang aan passende waarborgen voor de vertrouwelijkheid van deze gegevens – zeker wanneer deze persoonsgegevens met andere entiteiten kunnen worden gedeeld.

Ministeriële regeling

Het CBL heeft daarnaast kennis genomen van de bijgevoegde ministeriële (concept)regeling in de internetconsultatie. De maatregelen vermeld in de ministeriële regeling zijn van toepassing op bedrijven actief in de productie, verwerking en distributie van levensmiddelen. Het CBL constateert dat de zorgplicht zeer gedetailleerd is uitgewerkt met een grote hoeveelheid aan additionele vereisten.

Hierbij is voor het CBL niet altijd duidelijk welke uitgewerkte vereisten echt noodzakelijk zijn voor de cyberveiligheid van de essentiële dienstverlening. Het CBL vindt dan ook dat de nadere invulling van de zorgplicht zoals vermeld in de ministeriële regeling zich moet toespitsen op de belangrijkste vereisten direct gerelateerd aan de essentiële dienstverlening. Het CBL zou in de uitwerking graag nog meer een balans zien tussen enerzijds zorgvuldigheid en anderzijds administratieve lasten in de implementatie.

Overigens leest het CBL in de ministeriële regeling dat de drempelwaarden voor significante incidenten worden opgenomen. Hoewel bedrijven uiteraard voldoende op de hoogte moeten zijn van de drempelwaarden, zou overwogen kunnen worden om deze drempelwaarden vertrouwelijk met bedrijven te delen. Een openbare publicatie van de drempelwaarden kan gerelateerd zijn aan vertrouwelijke of concurrentiële informatie en kan bovendien kwaadwillende actoren onnodig informatie bieden.

Ten slotte leest het CBL in artikel 10 van de ministeriële regeling dat het begrip ‘asset’ wordt gebruikt, maar deze beperkt wordt gedefinieerd. In eerste instantie wordt assets gedefinieerd als ‘alles wat van waarde is voor het bedrijf’. De memorie van toelichting biedt verder verduidelijking dat het hier niet gaat om personeel of medewerkers en evenmin om financiële middelen. Omdat bedrijven worden geacht om een inventaris te hebben van de assets, zouden zij geholpen zijn met een verdere toelichting op het begrip assets, specifiek gericht op netwerk- en informatiesystemen.