Reactie CBL op de internetconsultatie Besluit weerbaarheid kritieke entiteiten

Het Centraal Bureau Levensmiddelenhandel (CBL), de koepelorganisatie van supermarkten en foodservicebedrijven, reageert via deze weg graag op de internetconsultatie van het Besluit weerbaarheid kritieke entiteiten. Het CBL pleit in het kort voor duidelijkheid en flexibiliteit, zodat de uitvoering praktisch en uitvoerbaar is voor de kritieke entiteiten die vallen onder de Wet weerbaarheid kritieke entiteiten.

Dubbele lasten voorkomen

Het CBL constateert dat sommige bedrijven in de levensmiddelenbranche kunnen vallen onder zowel de Wet weerbaarheid kritieke entiteiten (Wwke) als de Cyberbeveiligingswet. Beide wetten omvatten een zorgplicht en meldplicht voor respectievelijk de digitale veiligheid en de fysieke veiligheid. De Wwke voorziet erin dat een bedrijf dat onder de Wwke valt, automatisch ook onder de Cyberbeveiligingswet valt. Een bedrijf zou in dat geval te maken krijgen met een dubbele last: het zou moeten voldoen aan de verschillende documentatieverplichtingen onder zowel de Wwke als de Cyberbeveiligingswet. Volgens het CBL is deze dubbele last voor bedrijven onevenredig en draagt het niet per definitie bij aan een adequate digitale en fysieke veiligheid. Het CBL vindt daarom dat bedrijven onder de Wwke en de Cyberbeveiligingswet de mogelijkheid moeten krijgen om beide verplichtingen te verwerken in één gezamenlijke risicoanalyse en één maatregelenpakket. Ook de meldplicht voor bedrijven zou zoveel mogelijk geharmoniseerd moeten worden om dubbele lasten te voorkomen.

Fysieke beveiliging

Het CBL leest in artikel 8 van het voorliggende besluit dat kritieke entiteiten fysieke beveiligingsmaatregelen moeten nemen, zoals beveiligingszones, toegangscontrole en monitoring. Dit is volgens het besluit noodzakelijk om sabotage, diefstal en onbevoegde toegang te voorkomen. Hoewel het CBL de noodzaak inziet van fysieke beveiliging, ziet het CBL geen noodzaak om de praktische invulling hiervan wettelijk vast te leggen in deze vorm. Een doelgestuurde benadering zou volgens het CBL hier beter passen, omdat het betreffende bedrijf zelf de meeste inzichten heeft in de eigen beveiliging en de bijbehorende risico's. De risicobeoordeling kan hierbij worden betrokken. Een dergelijke risicogerichte benadering zou meer in lijn zijn met de oorspronkelijke CER-richtlijn.

Crisis- en continuïteitsplannen

Het CBL leest in artikel 9 van het besluit dat een kritieke entiteit moet beschikken over een crisismanagement- en bedrijfscontinuïteitsplan, deze toe moet passen en moet testen. Tegelijkertijd vindt het CBL het belangrijk dat bedrijven zelf de mogelijkheid moeten hebben om te kiezen hoe zij hun zorgplicht vastleggen. Het CBL wil voorkomen dat kritieke entiteiten te maken krijgen met een aanzienlijke, nieuwe rapportagedruk die niet per definitie bijdraagt aan de fysieke beveiliging. Daarom pleit het CBL ervoor dat kritieke entiteiten hier meer flexibiliteit in krijgen volgens hun eigen risicobeoordeling. Ook hier geldt dat deze risicogerichte benadering meer in lijn zou zijn met de oorspronkelijke CER-richtlijn.

Meldplicht

In artikel 15 van het Besluit leest het CBL dat de respectievelijke vakminister bij ministeriële regeling de drempelwaarden voor een aanzienlijke verstoring bekend worden gemaakt. Daarbij kan onderscheid worden gemaakt tussen sectoren, subsectoren en categorieën van entiteiten. Het CBL hecht eraan dat deze drempelwaarden vertrouwelijk worden gedeeld met de betreffende kritieke entiteiten. Het openbaar maken van deze drempelwaarden kan vertrouwelijke informatie betreffen en zou kwaadwillende actoren onnodig informatie kunnen bieden.