

Schriftelijke voorbereiding rondetafelgesprek Digitale Weerbaarheid d.d. 6 september 2022

Het CBL, de brancheorganisatie van supermarkten en groothandels, deelt in dit document haar visie op de digitale weerbaarheid van onze branche. Vaak wordt bij dit onderwerp als eerste gedacht aan de bescherming van werknemer- en klantgegevens of bijvoorbeeld phishing mail vanuit een supermarkt of groothandel. Wij willen echter graag de nadruk leggen op de backend van de bedrijven in onze branche, namelijk het logistieke proces.

Complexe logistieke operatie

De supermarkten en groothandels zijn geen vitale voorziening, maar zijn uiteraard wel van maatschappelijk belang gezien hun rol in de voedselvoorziening van Nederland. Om ervoor te zorgen dat de vier miljoen klanten die dagelijks in onze winkels komen hun boodschappen kunnen doen, werken supermarkten volgens een complex logistiek proces. Fabrikanten zorgen voor de aanvoer van producten bij één van de meer dan vijftig distributiecentra. Hier worden de producten geordend waarna vrachtwagens de juiste producten richting de supermarkten of online hubs vervoeren. De processen en informatiestromen van verschillende bedrijven zijn in deze keten steeds meer met elkaar verbonden. Het is dus van groot belang dat deze informatiestromen voldoende beveiligd zijn. Daarnaast is het voor de leden van het CBL van groot belang dat vitale infrastructuren, zoals het betalingsverkeer en het wegennet, goed beschermd zijn.

Belang van cyberveiligheid

Volgens de WHO is het aantal cyberaanvallen sinds COVID-19 verviervoudigd. De vraag hoe individuele supermarkten of groothandels met deze incidenten omgaan is niet eenduidig te beantwoorden. Dit is namelijk afhankelijk van de interne organisatiestructuur en het specifieke incident. Wel kan worden gezegd dat supermarkten het toegenomen dreigingsniveau van cybercriminaliteit zeer serieus nemen en volop investeren in preventieve en detective maatregelen om zo de continuïteit van bedrijfsprocessen te borgen. Cyberoefeningen kunnen onderdeel zijn van het interne beleid.

Het CBL ziet de volgende aandachtspunten als het gaat om de digitale weerbaarheid van Nederland:

- Het is momenteel niet helder wie de coördinatie op zich neemt bij een grootschalig incident. Heeft de overheid voldoende capaciteit (en specialiteit) in huis om een grote landelijke crisisstructuur op te zetten in tijden van crisis?
- Vooralsnog wordt het niet-vitale bedrijfsleven minimaal geïnformeerd over cyberkwetsbaarheden en dreigingen. Er loopt momenteel een pilot waarin de schaalbaarheid van een 'waarschuwingsdienst' van het Digital Trust Center wordt onderzocht. We hopen dat dit een vervolg krijgt en hier meer capaciteit en financiële middelen voor worden vrijgemaakt.
- Cyberveiligheid is geen onderwerp waarop bedrijven met elkaar willen concurreren. Er zou meer werk moeten worden gemaakt van een structuur waarin bedrijven van elkaar kunnen leren door eerdere casussen te bespreken.
- Het aanhoudende tekort aan gekwalificeerd IT-personeel blijft een groot probleem.

Tot slot

Zoals eerder aangegeven is de levensmiddelensector geen vitale sector. Door de NIS2-Richtlijn gaat onze branche in de toekomst tot de belangrijke bedrijven behoren en krijgen supermarkten en groothandels te maken met aanvullende regels. Het CBL hoopt dat er bij de implementatie van deze richtlijn in Nederlandse wetgeving gebruik wordt gemaakt van de kennis en expertise die aanwezig is bij het bedrijfsleven.

Bij het CBL zijn aangesloten:

Albert Heijn | Aldi | Bidfood | Boni Markten | Boon Food Group | Coop Supermarkten | Detailresult | Hoogvliet | Jan Linders | Jumbo Supermarkten | Lekkerland | Lidl Nederland | Makro Nederland | Nettorama | NS Stations Retail Bedrijf | PLUS Retail | Poiesz Supermarkten | Sligro | Spar | Vakcentrum | Groothandel in Levensmiddelen Van Tol | Vomar Voordeelmart |