CYBER-KETENWEERBAARHEID

Een verkennend onderzoek naar dreigingen, kwetsbaarheden en geleerde lessen

Doelstelling

Het krijgen van meer inzicht in het fenomeen cyber-ketenweerbaarheid in verschillende economische sectoren om daarmee de overheid te ondersteunen in advisering en ontwikkeling van beleid.

Onderzoeksvragen

1. Welke cyberspecifieke dreigingen ontstaan bij ketens en welke kwetsbaarheden spelen daarbij een rol?
2. Wat zijn geleerde lessen bij het voorkomen en bestrijden van cyberincidenten gerelateerd aan het opereren in een keten?

Methode

De onderzoeksvragen zijn beantwoord aan de hand van literatuuronderzoek en interviews. De interviews zijn uitgevoerd bij in totaal 12 bedrijven uit drie economische sectoren: agrarisch, sierteelt en handel. De bedrijven zijn binnen hun sector geschakeld (als afnemer en leverancier) en vormen daarmee een keten.

Conclusies

- **Ketens hebben last van specifieke dreigingen en kwetsbaarheden.** Met name ransomware en stepping stone-aanvallen zijn een dreiging. Een belangrijke kwetsbaarheid is technologie die op afstand kan worden bediend via internet door een derde partij, zoals klimaatregelaars en sorteersystemen.
- **Maatregelen gericht op de keten worden slechts sporadisch genomen.** Cyberveiligheid is veelal geen onderwerp in contracten met leveranciers, (structureel) overleg tussen partners op cybersecurity gebied blijft uit en informatiedeling over cyberrisico's en geleerde lessen op ketenniveau is beperkt.
- **De ene keten is de andere niet.** Verschillen in genoemde dreigingen, kwetsbaarheden en geleerde lessen tussen bedrijven zijn te verklaren door het type bedrijf en diens omvang, de volwassenheid van de organisatie op ICT-gebied en de positie van een bedrijf in de keten. Zo lijken met name ICT-dienstverleners en grote bedrijven zicht te hebben in en te handelen op keten-gerelateerde dreigingen en kwetsbaarheden
- **Hulp is nodig.** Ketens kunnen hulp gebruiken met het op orde brengen van de cyberveiligheid van de individuele partners, de cyberveiligheid tussen schakels en de cyberveiligheid van keten als geheel. Hierbij kan worden gedacht aan het beschikbaar stellen van voorbeeldcontracten met leveranciers, het faciliteren van (structureel) overleg tussen partners en ondersteuning van de informatiedeling op ketenniveau.

Lectoraat cybersecurity in het mkb
De Haagse Hogeschool

DE HAAGSE HOGESCHOOL