Door Hélène Minderman

DIGITALISERING BETEKENT BEVEILIGING VAN HET DIGITALE DOMEIN

NOODZAAK ADEQUATE CYBERSECURITY

Cybercrime vormt een actuele dreiging voor logistiek dienstverleners. De logistieke keten is kwetsbaar voor cybercriminaliteit en vormt een bedreiging voor de continuïteit van betrokken ondernemingen.

Er is al geruime tijd een verschuiving zichtbaar van klassieke naar digitale criminaliteit. Actief risicobeheer is noodzakelijk. In de huidige logistieke ketens is het verhogen van de digitalisering een prioriteit om te concurreren met concurrenten en het aansluiten op de wensen van de klant in de logistieke keten. Een keerzijde van het in hoog tempo digitaliseren in combinatie met de complexiteit van huidige logistieke ketens is dat er ook niet-fysieke aanvalsvlakken worden gecreëerd en er dus moet worden nagedacht over het beveiligen van het digitale domein: cybersecurity.

INTERESSANT DOELWIT

De afgelopen paar jaar is een aantal incidenten in het nieuws gekomen waaruit blijkt dat transport en logistiek een interessant doelwit is voor hackers en aanverwanten. Onderzoek wijst uit dat dit de komende decennia alleen maar vaker zal voorkomen. Daarnaast is Nederland een logistieke hotspot met haar perfecte ligging en infrastructuur. Nederland moet daarom voorop gaan lopen op het gebied van cybersecurity om nu en in de toekomst aantrekkelijk te blijven. Ruim 40 procent (bron: onderzoek Haagse Hogeschool) van de bedrijven in de logistieke sector heeft al eens te maken gehad met een vorm van cybercriminaliteit of hacking. Het niet meer kunnen vertrouwen op data of beschikbaarheid van systemen en applicaties, resulteert al snel in bedrijfsschade van tienduizenden euro's en verlies van klantvertrouwen.

BETERE CYBERSECURITY

TLN, SmartPort, Air Cargo Netherlands (ACN), Havenbedrijf Rotterdam, Cargonaut en Reqon Security gaan gezamenlijk met TNO door middel van een scan de kwetsbaarheden binnen de logistieke keten in kaart brengen. Daarmee zetten ze een volgende belangrijke stap in de verbetering van de cybersecurity van de keten. Het project moet het bewustzijn van het belang van cybersecurity verhogen en concrete handvatten bieden om de beveiliging tegen cybercrime te verbeteren. Het onderzoek wordt mede gefinancierd uit de Toeslag voor Topconsortia voor Kennis en Innovatie (TKI's) van het ministerie van Economische zaken.

DOE MEE MET HET TNO-ONDERZOEK

Cyberincidenten worden echter zwaar onderschat terwijl de gevolgen voor het logistieke proces zeer ingrijpend zijn. Ondernemers kunnen hun bedrijf in de logistieke sector helpen een stap voorwaarts te zetten in cybersecurity door de ontwikkelde vragenlijst in te vullen via https://tinyurl.com/cybercsl. Of maak gebruik van de QR-code onder aan deze pagina.

De vragenlijst geeft na iedere set van gemiddeld vier vragen een tip om de cybersecurity van een organisatie te verbeteren. Het invullen van de vragenlijst kan tot en met 31 juli 2019. De resultaten worden begin 2020 verwacht in de vorm van best practices en concrete handvatten om de cybersecurity van bedrijven in de logistieke keten te verbeteren. Deze worden via TLN verspreid.

Meer informatie over het consortium of het project? Stuur dan e-mail naar csl@tno.nl of naar hminderman@tln.nl.