CYBERSECURITY IN DE LOGISTIEKE KETEN

DE WEERBAARHEID EN UITDAGINGEN VAN DE LOGISTIEKE KETEN OP HET GEBIED VAN CYBERSECURITY

WAAROM

Het fysiek beveiligen van goederen en eigendommen is iets wat al eeuwen gebeurt. In de logistiek is elk terrein beveiligd met hekken, volgen medewerkers veiligheidsinstructies en wordt een belanghebbende aangemeld voordat hij of zij het terrein mag betreden.

De logistieke sector digitaliseert in rap tempo. Een keerzijde hiervan is dat er ook niet-fysieke kwetsbaarheden in de keten worden gecreëerd. Er zal moeten worden nagedacht over het beveiligen van het digitale domein: cybersecurity.

Interessant doelwit

Uit het aantal incidenten in het nieuws blijkt dat de logistiek een interessant doelwit is voor cybercriminelen. Voorbeelden laten zien dat de economische impact van een cyberaanval groot is. Veerkracht op gebied van cybersecurity mag niet onderschat worden.

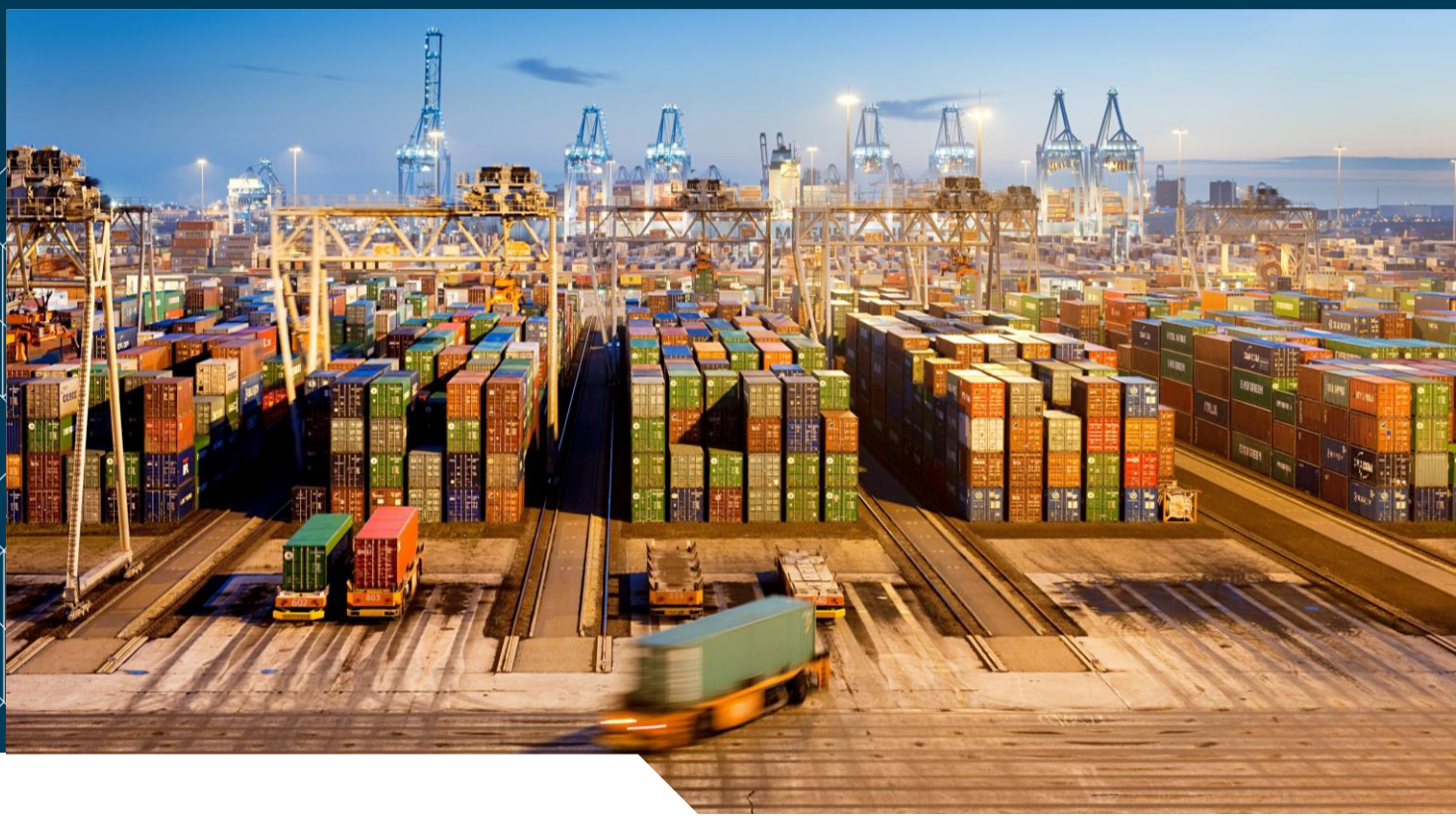
WAT

Er is behoefte aan een gestructureerde verkenning om de huidige stand van zaken op het gebied van cybersecurity in transport en logistiek in kaart te brengen. Deze uitdaging is aangegaan door een consortium bestaande uit TNO, TLN, ACN, SmartPort, Cargonaut, REQON Security, Computest en het Digital Trust Center.

Concrete handvatten

Cybersecurity vereist specifieke kennis en expertise die vaak ontbreekt bij logistieke dienstverleners. Middels tips en handvatten kunnen bedrijven zich laten helpen om hun niveau van cybersecurity te verhogen, maar vaak zijn deze tips niet specifiek voor de logistieke sector.

In dit project zijn concrete handvatten opgesteld specifiek voor logistieke dienstverleners die de gehele sector helpen beter voorbereid te zijn op de digitale dreigingen van nu en van de toekomst.



AUTEURS
Rik Poulus, TNO
Robin de Veer, TNO
Robert Wezeman, TNO

TKI DINALOG
Dutch Institute for Advanced Logistics

HOE

- **Inzicht verkrijgen hoe de logistieke sector ervoor staat op het gebied van cybersecurity.** Logistieke brancheorganisaties betrokken bij het consortium hebben een vragenlijst uitgezet onder hun leden. Daarnaast konden logistieke bedrijven meedoen aan een security assessment. Hierbij is een verdiepend interview afgenomen gecombineerd met de uitvoering van een ethische hack.
- **Cybersecurity handvatten gericht op de sector.** Opgedane inzichten zijn gecombineerd met inhoudelijke expertise vanuit andere sectoren om tot handvatten voor de logistieke sector te komen waarmee bedrijven hun cybersecurity kunnen vergroten.
- **Het creëren van bewustzijn van cybersecurity.** Door middel van webinars, publicaties en een vlog zijn de inzichten en handvatten verspreid naar de achterban van de consortiumpartners. Bij elk van deze activiteiten stond het verhogen van de bewustwording van het belang van cybersecurity centraal.

Uit het onderzoek blijkt dat 22% van de logistieke bedrijven tijdelijk niet heeft gefunctioneerd vanwege een cyberaanval, zoals ransomware. Visual: SmartPort

RESULTAAT

Het onderzoek laat zien dat er nog ruimte voor verbetering is op het gebied van cybersecurity in de logistieke sector.

- Veel bedrijven geven aan aandacht te besteden aan cybersecurity, maar desondanks wordt er veelal reactief gehandeld in plaats van proactief.
- Medewerkers zijn de belangrijkste bescherming, maar ook het grootste risico voor het bedrijf. Het bewustzijn onder medewerkers moet worden vergroot.
- Binnen de keten vindt nauwelijks samenwerking plaats op het gebied van cybersecurity.
- Bedrijven maken zich zorgen om de omgang met wachtwoorden en de fraudegevoeligheid van pincodes.

Visual: SmartPort

Handvatten

Om logistiek dienstverleners te helpen bij het verbeteren van hun cybersecurity zijn er handvatten opgesteld. Ieder bedrijf kan de handvatten gebruiken om de volgende stap te zetten, ongeacht de grootte van het bedrijf en de mate waarin al aandacht is besteed aan de digitale veiligheid. De handvatten zijn onderverdeeld in vier categorieën: beleid, bewustwording, ketenpartners en techniek. Bij elk handvat is een indicatie gegeven van de kosten en impact van de implementatie.

HOE VERDER

Logistieke (branche-)organisaties zoals TLN, ACN, SmartPort en Cargonaut nemen nu het voortouw om de opgedane lessen rondom cybersecurity te blijven verspreiden binnen hun achterban om zo het bewustzijn te laten groeien. Zij zullen de opgestelde handvatten via verschillende kanalen beschikbaar stellen aan de logistieke sector. Deze handvatten vormen een eerste stap naar een digitaal weerbaardere samenleving waarin we met z'n allen minder last ondervinden van uitval van logistieke dienstverlening.

Toekomst

Het huidige onderzoek kan beschouwd worden als een nulmeting van de cybersecurity weerbaarheid van de logistieke sector en leent zich daarmee om over drie tot vijf jaar herhaald te worden. Dit kan laten zien of de sector wakker is geschud en cybersecurity dan als proactief onderdeel in de bedrijfsvoering is opgenomen.

Maar ook in de toekomst zal onze hoofdboodschap blijven:
Logistieke sector, wapen je tegen cybercriminaliteit!

Het project is mede mogelijk gemaakt door TKI Logistiek / Dinalog en de Topsector Logistiek en gefinancierd door het Ministerie van Economische Zaken en Klimaat (EZK)