Cybersecurity in de logistie

Alle bedrijven in de logistieke keten moeten mee in de digitale transformatie om concurrerend te blijven. Een keerzijde van het in hoog tempo digitaliseren in combinatie met de complexiteit van huidige logistieke ketens is dat er ongewenste digitale kwetsbaarheden ontstaan. Cybercriminaliteit is één van de bedreigingen voor de continuïteit van bedrijven in logistieke ketens. TLN, SmartPort, Air Cargo Netherlands (ACN), Havenbedrijf Rotterdam, Cargonaut en REQON Security werken gezamenlijk met TNO aan de verbetering van cybersecurity van hun logistieke ketens.

Om een concurrerende positie te verkrijgen en te kunnen behouden heeft de logistieke sector een groot deel van haar activiteiten moeten digitaliseren. Een groeiend aantal IT-systemen wordt gebruikt voor communicatie, het delen van informatie en het plannen van activiteiten. Deze ontwikkelingen geven veel voordelen, maar er is ook een toenemend risico. De systemen zouden kunnen uitvallen door een storing of door de groeiende dreiging van cybercriminaliteit. Een concreet voorbeeld van een cyberaanval met impact op de logistieke sector is de uitval van de APMT Maersk containerterminal door een ransomware-aanval (*1). Door deze aanval hebben de terminaloperaties enkele dagen stil moeten liggen met als gevolg miljoenen euro's aan schade. Naast de directe impact wereldwijd op de operaties van Maersk had deze aanval ook een groot effect op alle operaties in de Rotterdamse haven, een duidelijk voorbeeld van een enkel storingspunt dat het grotere systeem beïnvloedt. In het ergste geval kunnen containers niet worden ingeklaard. Al naar gelang de inhoud van die containers heeft dat mogelijk grote gevolgen voor de economie en het welzijn van mensen.

Bestendigheid Een consortium bestaande uit TLN, SmartPort, Air Cargo Netherlands (ACN), Havenbedrijf Rotterdam, Cargonaut, REQON Security en TNO onderzoekt met een gestructureerde verkenning de huidige stand van zaken op het gebied van cybersecurity in transport en logistiek en doet voorstellen voor verbetering op dit vlak. Om de cyberverstoringen in logistieke ketens te voorkomen, is over de gehele keten een behoorlijk niveau van cyberbestendigheid vereist. Logistieke ketens zijn gevoelig voor de volgende typen cyberaanvallen, al dan niet in combinatie met elkaar.

- Distributed Denial of Service: een systeem (bijvoorbeeld een website) wordt door het genereren van veel communicatieverkeer zodanig overbelast dat het systeem effectief niet meer beschikbaar is.
- Phishing attacks: door middel van bijvoorbeeld phishing e-mails met daarin een link waarop wordt geklikt, worden computers besmet met malware en kan informatie worden gestolen of de besturing van computers en netwerken volledig worden overgenomen.
- Hacken: het gebruik maken van zwakheden in systemen (bijvoorbeeld slecht geïmplementeerde websites) waardoor ongeautoriseerde toegang wordt verschaft en informatie kan worden gestolen of de besturing van systemen en netwerken kan worden overgenomen.
- Malware: kwaadaardige software die gemaakt is om informatie of informatie over identiteiten te stelen of om de besturing van systemen over te nemen.
- Ransomware: een specifieke vorm van malware, waarbij alle informatie op een systeem wordt versleuteld zodat deze niet meer bruikbaar is. Meestal wordt dan een 'losgeld' geëist om de informatie weer bruikbaar te maken.

Fysieke beveiliging Het fysiek beveiligen van goederen en eigendommen is iets dat al eeuwen gebeurt. In de logistiek is elk terrein beveiligd met grote hekken, veiligheidsinstructies, een aanmelding voordat een belanghebbende het terrein mag betreden en stringente controle op de uitgaande goederenstromen. Containers zijn verzegeld om te controleren of er mogelijke frauduleuze handelingen zijn geweest.
Een keerzijde van het in hoog tempo digitaliseren is dat er ook niet-fysieke aanvalsvlakken zijn gecreëerd. Logistieke ketens hebben een aantal unieke kenmerken waardoor cybersecurity een uitdaging is in de praktijk. Zo is bijvoorbeeld de heterogeniteit van de bedrijven in de keten groot: veel verschil qua grootte bedrijf en type bedrijf (expediteur, producent of vervoerder). De marges zijn over het algemeen laag, waardoor beveiliging in het algemeen niet de hoogste prioriteit heeft. Mede door de complexiteit (veel schakels) is het lastig om een goed overzicht te hebben van de handelingen van mens, machine en organisatie. Het schort aan bewustzijn in de keten van de bestaande risico's op het gebied van cybersecurity. Dit ligt mede aan de IT-budgetten van veel bedrijven. Deze zijn met name bedoeld om interne bedrijfsprocessen te digitaliseren en minder op het gebied van security met mogelijk grote maatschappelijke schade als gevolg. Naast de bestaande risico's binnen de bedrijven in de logistieke keten zijn er risico's aangaande de interface/koppe-

ke keten

ling met het volgende bedrijf in de logistieke keten. Dit is zeker nog een aspect dat qua cybersecurity extra aandacht verdiend en op dit moment nog onderbelicht is.

Onderzoek Het consortium werkt aan de verbetering van cybersecurity. Om gepast advies te kunnen geven dient de huidige staat van de cybersecurity in de logistieke keten bekend te zijn. Middels vragenlijsten, interviews en enkele ethische hacks bij verschillende logistieke bedrijven in de Rotterdamse haven zal een eerste beeld worden gevormd waar de sector het meest kwetsbaar is.
Het doel van het gezamenlijke onderzoek is om een gestructureerde eerste verkenning van de huidige stand van zaken op gebied van de cybersecurity in transport en logistiek in kaart te brengen. Uit de eerste resultaten blijkt dat er een daadwerkelijke behoefte is aan hulp op gebied van cybersecurity. In dit onderzoek richt het consortium zich op zaken als de bewustheid van de dreiging en het hebben van een digitaal rampenplan. Ook wordt er gekeken naar technischere zaken zoals welke beveiligingsstandaarden worden gebruikt, hoe de toegangscontrole is geregeld binnen IT-systemen en de manier waarop wordt omgegaan met kritische data.
In dit onderzoek worden zowel kleine, gemiddelde als grote bedrijven benaderd. De verwachtingen zijn dat voor de kleine logistieke bedrijven nog veel te winnen valt op het gebied van cybersecurity. Gezien de gezamenlijke verantwoordelijkheid voor een cyberweerbare keten, wordt geprobeerd middels het organiseren van events en seminars deze partijen aan te zetten tot kennisoverdracht aangaande cybersecurity.

Best practices Aan de hand van de resultaten worden best practices opgesteld die gedeeld worden met de deelnemende partijen. Het onderzoek is in eerste instantie een nulmeting. De mogelijkheid bestaat om de stand van zaken in een mogelijk vervolgonderzoek over enkele jaren te herhalen. Aan de hand van resultaten van een vervolgonderzoek kunnen dan conclusies getrokken worden of de logistieke sector zich snel genoeg aanpast aan de nieuwe cyberdreigingen van de toekomst.

■ Ir. Geert Kleinhuis, Rik Poulus MSc, Robert Wezeman MSc
Werkzaam bij TNO
Geert.Kleinhuis@tno.nl, Rik.Poulus@tno.nl, Robert.Wezeman@tno.nl

***1) https://tweakers.net/nieuws/128411/aanval-met-notpetya-malware-kost-maersk-tot-256-miljoen-euro.html**

Onderzoek

Zou uw bedrijf geholpen willen worden op het gebied van cybersecurity?	85%
Door middel van een informatieve website	42%
Door middel van een scan die bedrijf doorlicht op technische zwakheden	39%
Door middel van een mystery guest (*1)	26%
Door middel van ethische hack	39%
Door middel van een lijst met belangrijkste dreigingen	41%

De percentages geven aan welk deel van de respondenten de vraag met ja hebben beantwoord.

***1) Een mystery guest is een social engineer die zich voordoet als een normale bezoeker, met als doel het uitbuiten van kwetsbaarheden in de beveiliging.**