EINDRAPPORTAGE

CYBER SECURITY IN LOGISTICS

J.W. DE VRIES, R. WEZEMAN & R. DE VEER

TKI DINALOG
Dutch Institute for Advanced Logistics

SAMENVATTING

Het consortium van Cyber Security in Logistics is een samenwerkingsverband met als doel het bewustzijn over cybersecurity in de transport- en logistieke sector te verhogen. Op basis van interviews en uitgevoerde ethische hacks zijn concrete handvatten geformuleerd om te helpen de beveiliging van de sector tegen cybercrime te verbeteren.
Vanuit het onderzoek komen concrete aanbevelingen naar voren:

• **Stel een cybersecurity verantwoordelijke aan**. Er zijn bedrijven waarbij een fulltime Chief Information Security Officer (CISO) wordt aangesteld, maar cybersecurity kan ook als taak worden belegd bij een (IT-)medewerker. Vaak is de invulling afhankelijk van de bedrijfsgrootte en de bedrijfstak.
• **Zet het onderwerp cybersecurity op de agenda van vergaderingen**. Zorg dat er tijdens vergaderingen regelmatig aandacht wordt besteed aan cybersecurity. Doe dit niet reactief, maar proactief. Voorbeelden van wat besproken kan worden: rapporteren actuele situatie en lopende beveiligingsacties aan directie/management, bewustzijn onder medewerkers, etc.
• **Maak een cybercrisisplan en test het plan regelmatig.**
• **Automatiseer het maken van back-ups.**
• **Zorg dat patches en updates tijdig worden uitgevoerd**. Voor een goede beveiliging is het tijdig uitvoeren van software patches of updates van groot belang. Zorg dat er een duidelijk overzicht is van de beschikbare en laatste uitgevoerde patches en updates.
• **Richt processen in rondom de in-en uitdiensttreding van personeel en automatiseer deze processen indien mogelijk.**

Inzichten uit onderzoek: Cybersecurity en de logistieke sector

Aandachtpunten
In zijn algemeenheid vraagt het consortium in het onderzoek aandacht voor de volgende punten:
• Cybercrime vormt (ook) een actuele dreiging voor logistiek dienstverleners. Wees bewust van de mogelijke risico's en bedrijfsschade die door deze nieuwe dreigingen kan ontstaan;
• Investeer in adequate IT- en informatiebeveiliging/gegevensbescherming zodat digitale productiemiddelen goed beschermd zijn en je de risico's van cybercriminaliteit beperkt;
• Bereid de organisatie voor op het goed reageren en afhandelen van incidenten. Dat stelt jouw bedrijf in staat om schade als gevolg van cybercriminaliteit te beperken en de continuïteit van de bedrijfsvoering te waarborgen.

INHOUDSOPGAVE

DE URGENTIE ONTBREEKT. LOGISTIEKE SECTOR: WAPEN JE TEGEN CYBERCRIMINALITEIT!

JANNEKE DE VRIES
PROJECTMANAGER DUURZAME LOGISTIEK

AANLEIDING

Cybercriminaliteit vormt een steeds groter gevaar voor ondernemers, ook voor transport- en logistieke ondernemers. Het leidt jaarlijks tot meer dan € 10 miljard schade aan de Nederlandse economie. Het consortium van Cyber Security in Logistics roept alle logistiek dienstverleners op om zich beter te wapenen tegen deze vorm van criminaliteit die de afgelopen jaren explosief gestegen is.

Het belang van de veiligheid van digitalisering in de logistieke sector

Het aantal gevallen van cybercrime stijgt dit jaar enorm, met maar liefst 169 procent vergeleken met vorig jaar, zo meldt de politie in haar **halfjaarcijfers** van 2020. In het eerste kwartaal van dit jaar registreerde de politie bijna 2800 cybercrime-misdrijven in Nederland. Dat is in vier maanden tijd al bijna net zoveel als in heel 2018.

De keerzijde van digitalisering

Digitalisering is een steeds belangrijker onderdeel van de huidige logistieke ketens, denk aan digitale documentuitwisseling, gebruik van online boekingsplatformen, het automatisch inschieten van orders, digitale planningen en afhandeling van transacties. Door de hoge eisen van klanten van leveranciers en logistiek dienstverleners voor tijden van levering, ligt er een grote druk op het efficiënt inrichten van de logistieke keten en de bijbehorende informatievoorziening. De digitalisering zorgt ervoor dat aan de wensen van de klant kan worden voldaan en dat je daarmee een betrouwbare partner in de keten blijft. Een keerzijde van het in hoog tempo digitaliseren van de logistieke keten is dat criminaliteit zich verplaatst naar de digitale wereld. Bovendien worden cybercriminelen steeds professioneler en gebruiken ze steeds geavanceerdere en verfijnde technieken. Dit betekent dat er ook in de logistieke sector goed nagedacht moet worden over de digitale veiligheid, de zogenaamde cybersecurity.

Logistiek als doelwit

De afgelopen paar jaar zijn diverse cybersecurity incidenten in het nieuws gekomen waaruit blijkt dat transport en logistiek een interessant doelwit is voor cybercriminelen. Daarnaast is Nederland een logistieke hotspot met haar perfecte ligging en infrastructuur. Echter mist op het moment inzicht in de volwassenheid van de logistieke sector op het gebied van cyberveiligheid en de huidige stand van zaken wat betreft de kwaliteit van cyberveiligheid bij de partijen.

Onderzoeksproject Cyber Security in Logistics

Een consortium bestaande uit TNO, TLN, ACN, Cargonaut, Computest & SmartPort gaan deze uitdaging aan, te beginnen met inzicht verkrijgen in de huidige stand van zaken met betrekking tot cybersecurity en de bewustwording te creëren. Dit TKI-project focust zich op • het creëren van meer cybersecurity-bewustzijn op het gebied van logistiek bij bedrijven, • beter inzicht in de gevaren en bedreigingen die spelen op dit gebied in de logistieke sector en • inzicht in de mate van volwassenheid die de logistieke sector heeft op het gebied van cybersecurity ten opzichte van andere sectoren.

UITDAGING

De logistieke sector is en is steeds meer van haar activiteiten gaan digitaliseren. Een groeiend aantal IT-systemen wordt gebruikt voor communicatie, het delen van informatie of het plannen van activiteiten, benodigd voor het efficient bezorgen van goederen. Er zijn veel voordelen van deze ontwikkelingen, maar er is ook een toenemend risiconiveau. De systemen zouden kunnen uitvallen, door een storing of door de groeiende dreiging van cybercriminaliteit. Om de veiligheid en continuïteit van alle logistieke operaties te waarborgen, moeten logistieke bedrijven een behoorlijk niveau van cyberbeveiliging hebben. De logistieke ketens hebben een aantal unieke kenmerken waardoor cybersecurity een uitdaging is in de praktijk, namelijk de heterogeniteit bij de bedrijven onderling is groot (veel verschil in grootte bedrijf, type bedrijf(expediteur, producent, vervoerder). De marges zijn over het algemeen laag, waardoor security over 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.

In dit onderzoeksproject zijn - op basis van een enquete onder 200 logistiek dienstverleners, interviews en uitgevoerde ethische hacks - concrete handvatten geformuleerd om te helpen de beveiliging van de sector tegen cybercrime te verbeteren.

PROJECTOPZET

TNO, Transport en Logistiek Nederland (TLN), SmartPort, Air Cargo Netherlands (ACN), Cargonaut, REQON Security, Computest en Topsector Logistiek hebben een scan uitgevoerd om de cyber kwetsbaarheden binnen de logistieke keten in kaart brengen. Het onderzoek is mede gefinancierd uit de Toeslag voor Topconsortia voor Kennis en Innovatie (TKI's) van het ministerie van Economische zaken.

Doelstelling van het project is verhogen van het bewustzijn van het belang van cybersecurity en bieden van concrete handvatten om de beveiliging tegen cybercrime te verbeteren.

De huidige status van cybersecurity in de logistieke keten is in kaart gebracht middels:

- Een vragenlijst uitgezet door meerdere logistieke brancheorganisaties
- Interviews met verschillende soorten logistieke bedrijven
- Ethische hacks waarbij een ransomware-aanval is gesimuleerd zodat deelnemende bedrijven inzicht krijgen in de cyberveiligheid van hun IT

De best practices in dit document komen voort uit de resultaten van de bovengenoemde onderdelen.

1

WP1: INZICHT IN DE STATUS VAN CYBER RESILIENCE

Door middel van een enquête en verdiepende interviews worden inzichten opgedaan in de status van cyber resilience bij vervoerder en verladers. Deze inzichten worden overzichtelijk samengevat.

2

UITVOEREN ACTIES VOOR HET CREËREN VAN BEWUSTZIJN VAN VERVOERDERS EN VERLADERS OP HET ONDERWERP CYBER SECURITY

Uitvoeren acties voor het creëren van bewustzijn van vervoerders en verladers op het onderwerp cyber security.

3

DISSEMINATIE HANDVATTEN SECTOR

Beschikbaar maken en verspreiden van de onderzoeksresultaten naar TLN en EVO-leden middels inspiratiesessies, kennisoverdracht, informatiebrochures, websitecontent en lezingen.

4

PROJECTMANAGEMENT

Project management van het TKI-project, afstemming met TKI Dinalog en zorg dragen voor project reporting,
voortgangsbijeenkomsten,
eindrapportage en financiele
rapportages
opleveren

Inzichten onderzoek: Dreiging in de Logistieke Sector

RESULTATEN

Het onderzoeksproject Cyber Security in Logistics heeft als doel de status van cyberveiligheid in de logistiek te testen en het bewustzijn over cybersecurity in de transport- en logistieke sector te verhogen. De resultaten van de interviews laten onder andere zien dat 82% van de bedrijven schat in dat de medewerkers zich bewust zijn van de risico's op het gebied van cybersecurity. Echter schat maar de helft de bedrijven (54%) in de dat de medewerkers ook naar deze risico's kunnen handelen. Daarnaast valt ook op dat Cybersecurity is bij meer dan de helft van de bedrijven gespreksonderwerp bij overleggen. Ook vanuit een technisch oogpunt is de veiligheid van de IT-omgeving van verschillende logistiek dienstverleners bekeken. Hier is onder andere gekeken naar de ingeregelde rollen op netwerkshares, patchniveau, netwerkscheiding en de kwaliteit van de default wachtwoorden. Resultaten laten zien dat op al deze punten minstens 60% de bedrijven ondermaats presteerden. De status van de cyberveiligheid staat in schril contrast met de mate waarin bedrijven bevestigen na te denken over hun cyberveiligheid. De resultaten van de ethische hacks bevestigen de eerder geformuleerde hypothese dat – gezien de kleine marges en IT-budgetten in de logistieke sector – de cyberveiligheid van logistiek dienstverleners nog wat aandacht behoeft.

Op basis van de enquête, interviews en uitgevoerde ethische hacks zijn concrete handvatten geformuleerd om te helpen de beveiliging van de sector tegen cybercrime te verbeteren. Deze handvatten zijn te categoriseren onder: Beleid, ketenpartners, bewustwording en techniek.
Hieronder volgt een kleine greep (voor meer informatie verwijs ik u graag door naar het rapport 'Handvatten'):

- **Maak een cybercrisisplan en test het plan regelmatig.**
- **Automatiseer het maken van back-ups.**
- **Zorg dat patches en updates tijdig worden uitgevoerd**.
- **Richt processen in rondom de in-en uitdiensttreding van personeel en automatiseer deze processen indien mogelijk.**

MAATSCHAPPELIJKE RESULTATEN	
CO2 reductie	Nvt
Kostenbesparing	Nvt
Vermeden vervoerskilometers	Nvt
Modal shift tonkilometers	Nvt
Andere resultaten	Bewustzijn voor urgentie verbetering cyberveiligheid

SECTOR RESULTATEN	
Gecreëerde toegevoegde waarde	Bewustzijn in cyberveiligheid
Gecreëerde duurzame arbeidsplaatsen	Nvt

Het project Cybersecurity in de logistiek heeft een bijdrage geleverd aan 1 of meer Smart ICT KPI's van NLIP.

- KPI 1: 90% van alle platforms (PCS/BCS) in de Nederlandse supply chain wisselen logistieke data uit via NLIP.
- KPI 2: 100 apps maken gebruik van NLIP data.

Het project cybersecurity in de logistiek levert vooral een bijdrage aan KPI 1 van Smart ICT. Door inzicht te verschaffen over de cyber resilience van een drie tal in het project te definiteren logistieke ketens en samen met de deelnemende partijen acties te bepalen voor o.a. het verhogen van het bewustzijn met betrekking tot cybersecurity in de logistieke keten wordt aan KPI 1 een duidelijke bijdrage geleverd. Gedurende het project zal partner Cargonaut de kennis gebruiken om het eigen community platform meer cyber resilient te maken.

Bereikte bedrijven	300
Bereikte MKB bedrijven	200
Onderzoekers/ studenten nu werkzaam bij bedrijven	0

WETENSCHAPPELIJKE OUTPUT	
Master thesis	0
PhD promoties	0
Wetenschappelijke publicaties	0
Citations wetenschappelijke publicaties	0
Wetenschappelijke seminars, workshops, presentaties etc.	0

Resultaten van het onderzoeksproject zijn

RESULTATEN WAAR HET PROJECT TROTS OP IS

1. DE SAMENWERKING VAN HET DIVERSE CONSORTIUM IS EEN VOORBEELD HOE DOOR KRACHTEN EN INZICHTEN TE BUNDELEN WAPENEN BETER GEWAPEND KAN WORDEN TEGEN CYBERCRIME IN DE LOGISTIEKE KETEN.
2. DE ZICHTBAARHEID EN HET BEREIK VAN HET PROJECT. DE GEORGANISEERDE WEBINARS ZIJN GOED BEZOCHT, JUIST IN DE TIJDEN VAN CORONACRISIS.
3. BEWUSTBAARHEID DIE GECREEERD IS BIJ DE AAN DE ETHISCHE HACK DEELGENOMEN LOGISTIEKE PARTIJEN. DEZE BEWUSTBAARHEID MOET ZICH DOOR DE KETEN VERDER GAAN VERSPRIJDEN.
4. DE OPGELEVERDE HANDVATTEN GEVEN CONCRETE STAPPEN DIE VOOR LOGISTIEKE PARTIJEN DIRECT TOEPASBAAR ZIJN.
5. DUIDELIJK BEELD WAT GEVORMD IS OVER DE HUIDIGE STAAT EN WAAR KANSEN LIGGEN VOOR CYBERSECURITY IN DE LOGISTIEKE KETEN. OOK HIER GELDT, METEN IS WETEN.
6.
7. -
8. -
9. -
10. -

TITEL TOOL / DEMONSTRATOR 1

Niet van toepassing voor het project Cyber Security in Logistics

Onderschrift van een foto

TITEL TOOL / DEMONSTRATOR 2

Niet van toepassing voor het project Cyber Security in Logistics

Onderschrift van een foto

ERVARINGEN

Het project kende een vliegende start waarin een enquite is uitgezet bij de achterban van de logistieke consortium partners. Het bleek echter een enorme uitdaging om genoeg respons te krijgen van logistieke partijen, zowel bij de enquite als bij de ethische hacks. Dit is in lijn met onze bevindingen, er wordt binnen de logistieke sector voornamelijk reactief gehandeld op gebied van cyber security in plaats van proactief. Om toch tot voldoende deelnemers te komen heeft het project vertraging opgelopen. Desondanks de vertraging is uiteindelijk een duidelijk beeld gevormd van de huidige status van cybersecurity in de logistieke keten en zijn er concrete handvatten opgesteld en zijn diseminatie activiteiten goed bezocht geweest.

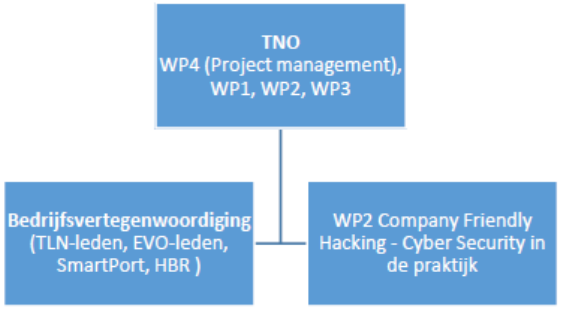
OPEN INNOVATIE

De valorisatie en implementatiestrategie werd vormgegeven in lijn met de werkzaamheden van WP4 (Disseminatie en valorisatie). TLN, ACN, Cargonaut & Smartport hadden de sleutel in handen wat betreft kennisdeling. Daarbovenop geldt dat de projectpartners beogen de ontwikkelde kennis te delen in de praktijk tijdens en na afronding van het project.

Een van de kerntaken van TLN, ACN en Smartport is kennisdeling en het publiek maken van resultaten en presentaties. Zo is in samenwerking met TLN twee webinars georganiseerd om het onderwerp Cyber Security meer op de kaart te zetten. SmartPort heeft het initiatief getoond om een vlog te organiseren; van communicatieplan, tot contact met alle betrokken belanghebbenden en de uitvoering. Deze vlog zal via verschillende kanalen van TLN, ACN en Smartport worden gedeeld.

DINALOG EN TOPSECTOR LOGISTIEK

De projectorganisatie van Cybersecurity in de logistiek is georganiseerd met TNO als penvoerder en werkzaam binnen WP1, 2 en 3. Daarnaast is TNO verantwoordelijk voor het betalingsschema dat opgesteld is na goedkeuring van het TKI-project. De bedrijfspartners in het consortium stellen mensen, kennis en resources ter beschikking voor werkpakketten WP1, WP2 en WP3. De bedrijfspartners hebben ook – als bijdrage aan de activiteiten in WP2 – deelnemers voor interviews en friendly hacks benaders. In totaal zijn 200 logistiek dienstverleners benaderd om de interviews uit te voeren.



Figuur 2. Projectorganisatie

TNO

TNO is penvoerder en overall trekker WP1, WP2, WP3 en WP4. De specifieke van TNO is de inbreng van cybersecurity kennis vanuit het cyber security shared research programma. Daarnaast brengt TNO kennis in over de logistieke keten en logistieke concepten.

Onderschrift bij een foto

TLN

TLN is trekker eigen disseminatie handvatten in de sector (WP3) en bijdrage in kennis en ervaring in alle WP’s. Zij brengen kennis in met betrekking tot programma veilig zakelijk internet, TAPA en VBN. Zij hebben contacten in de logistieke keten voor interviews en voor de hack in de keten.

Onderschrift bij een foto

TOEKOMSTVISIE

Cybersecurity gaat een steeds belangrijkere component worden van de bedrijfsvoering, juist binnen een snel digitaliserende keten zoals de logistieke sector. Het is belangrijk dat bedrijven realiseren dat het nu de tijd is om proactief te gaan handelen in plaats van reactief. De resultaten van dit onderzoek bieden logistieke bedrijven concrete handvatten om zich als keten beter te wapenen tegen cybercrime. Logistieke (branche-) organisaties zoals TLN, ACN, DTC, SmartPort en Cargonaut hebben nu het voortouw om de opgedane lessen rondom cybersecurity te blijven verspreiden aan hun achterban om zo het bewustzijn te doen groeien maar ook te behouden.
Extra bewustzijn zal leiden tot minder schade en minder uitval van logistieke dienstverlening. Met als resultaat een betrouwbaardere en veiligere samenleving.
In het huidige onderzoek is een nul meting gedaan van de cyberweerbaarheid in de logistieke sector. In een wat verdere toekomst, zeg 3 jaar, zou opnieuw een spreekwoordelijke thermometer in de sector gehangen kunnen worden om deze te vergelijken met de inzichten uit het huidige onderzoek. Het is leerzaam om te zien of de sector wakker is geschud en er daadwerkelijk vooruitgang is geboekt op gebied van cybersecurity. Juist dit soort inzichten kan helpen bij de ernst van cybersecurity op de kaart te zetten.

Logistiek dienstverleners: Ga aan de slag met je cyberveiligheid op basis van de handvatten van dit onderzoek.

VERVOLGACTIVITEITEN

Zoals eerder genoemd is een van de vervolgactiviteiten om de opgedane inzichten en verkregen handvatten te versprijden aan logistiek Nederland. Het doel is hier om het bewustzijn van het belang van cybersecurity te vergroten, dit zal gedaan worden door periodieke nieuwsberichten, artikelen en vlogs.

Naast deze disseminatie zijn ook andere (parallele) initatieven onstaan om de cybersecurity van de logistiek of ketens te onderzoeken, hiervan lichten we twee uit;

- TNO voert een onderzoek uit voor het Ministerie van Infrastructuur en Waterstaat naar ontwikkelingen en de stand van zaken rond cybersecurity van schepen. Het onderzoek bestaat uit twee onderdelen; een cybersecurity handreiking voor de Nederlandse scheepvaartsector, en een (geaggregeerde) inventarisatie van de sector op het onderwerp cybersecurity.
- Cybersecurity in de agrarische sector. In dit onderzoek wordt vergelijkbaar als in dit onderzoek de ketensamenwerking op gebied van cybersecurity onderzocht in de agrarische sector. Bij dit onderzoek is TNO niet betrokken.

Het is interssant om de verkregen resultaten te vergelijken met de resultaten uit de bovengenoemde onderzoeken. Door opgedane inzichten en geleerde lessen met elkaar delen zorgen we voor een hogere cyberweerbaarheid van verschillende ketens in Nederland.

CYBERSECURITY GAAT EEN STEEDS BELANGRIJKERE COMPONENT WORDEN VAN DE BEDRIJFSVOERING, JUIST BINNEN EEN SNEL DIGITALISERENDE KETEN ZOALS DE LOGISTIEKE SECTOR.

JANNEKE DE VRIES
PROJECTMANAGER DUURZAME LOGISTIEK

PROJECT PARTNERS

-

PUBLIEKE PARTNERS

TNO

TNO is penvoerder en overall trekker WP1, WP2, WP3 en WP4. De specifieke van TNO is de inbreng van cybersecurity kennis vanuit het cyber security shared research programma. Daarnaast brengt TNO kennis in over de logistieke keten en logistieke concepten.

DIGITAL TRUST CENTER (DTC)

Sinds eind 2017 bestaat ook het Digital Trust Center (DTC), opgericht om vooral de niet-vitale sector te ondersteunen ophet gebied van cybersecurity. DTC brengt kennis in over de status van cyberveiligheid en vernieuwde inzichten en tools over cyberveiligheid in de logistieke keten.

NAAM PARTNER

Omschrijving partner: beschrijving organisatie en rol en specifieke inbreng expertise in het project

NAAM PARTNER

Omschrijving partner: beschrijving organisatie en rol en specifieke inbreng expertise in het project

NAAM PARTNER

Omschrijving partner: beschrijving organisatie en rol en specifieke inbreng expertise in het project

NAAM PARTNER

Omschrijving partner: beschrijving organisatie en rol en specifieke inbreng expertise in het project

NAAM PARTNER

Omschrijving partner: beschrijving organisatie en rol en specifieke inbreng expertise in het project

NAAM PARTNER

Omschrijving partner: beschrijving organisatie en rol en specifieke inbreng expertise in het project

PRIVATE PARTNERS

TLN

TLN is trekker eigen disseminatie handvatten in de sector (WP3) en bijdrage in kennis en ervaring in alle WP's. Zij brengen kennis in met betrekking tot programma veilig zakelijk internet, TAPA en VBN. Zij hebben contacten in de logistieke keten voor interviews en voor de hack in de keten.

ACN

ACN is trekker eigen disseminatie handvatten sector WP3 en bijdrage in alle WP's. Zij brengen logistieke contacten in de keten in (leden, hubs, etc) en kennis over de cybersecurity status bij aangesloten bedrijven vanuit het platform CYSSEC.

SMARTPORT

SmartPort is trekker eigen disseminatie handvatten in de sector WP3 en bijdrage aan alle WP's. Zij brengen een afstudeeronderzoek over de status van cyber preventie in de havenlogistiek. Deze informatie zal na goedkeuring van Steven Lak ingebracht worden. Inbreng van logistieke contacten voor een goede doorsnede van de logistieke keten.

REQON

REQON is trekker in WP2 van het friendly hack onderdeel. Zij brengen technische kennis in van cybersecurity in de logistieke keten.

CARGONAUT

Zij zijn trekker eigen disseminatie handvatten in de sector van WP3 en bijdrage aan alle WPs. Zij brengen logistieke contacten in de keten in en kennis over de cybersecurity status bij aangesloten bedrijven en vanuit het platform CYSSEC.

COMPUTEST

Computest is betrokken geweest in WP2 bij het verwerken en analyseren van resultaten van de ethische hack. Zij brengen technische kennis van cybersecurity in de logistieke keten.

-

NAAM PARTNER

Omschrijving partner: beschrijving organisatie en rol en specifieke inbreng expertise in het project

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).

TKI DINALOG
Graaf Engelbertlaan 75
4837 DS Breda

info@dinalog.nl
www.dinalog.nl
+31 (0)76 531 53 00

TKI Dinalog is een uitvoeringsorganisatie van de Topsector Logistiek