



VEILIGE LOGISTIEKE KETEN CRUCIAAL VOOR VEILIG VESTIGINGSKLIMAAT

GEVAAR DREIGT VOOR REPUTATIE BV NEDERLAND

Een onveilige keten betekent een concreet gevaar voor de internationale reputatie van Nederland. Wanneer Nederland onveilig is voor transport en logistiek, dan kiezen ladingbelanghebbenden voor routes die niet via Nederland lopen.

Ondermijnende criminaliteit is bedrijfslevenbreed en ook in de transport- en logistieke sector een groot probleem. Criminelen misbruiken de logistieke keten voor de handel in illegale goederen voor de criminele industrie. Dit gaat ten koste van de internationale reputatie van Nederland en trekt allerlei criminele netwerken en activiteiten aan, wat ervoor zorgt dat het ondermijningsprobleem zich vergroot. Een onveilige sector zorgt ervoor dat Nederland zijn positie als 'gateway to Europe' verliest.

KEUZE VOOR SECURITY

Security draagt bij aan het succes van de onderneming. Klanten worden steeds bewuster en kiezen daardoor vaker voor een bedrijf waar securitymaatregelen zijn genomen. Supplychainsecurity richt zich op het nemen van beveiligingsmaatregelen ten behoeve van de gehele logistieke keten. Beveiligingsmaatregelen zorgen voor veilig produceren, opslaan en vervoeren van goederen. Het uitgangspunt is de beveiliging van de hele keten, dus van producent tot afnemer. Het doel is te voorkomen dat

goederenstromen worden misbruikt door criminelen en terroristen.

Een veilige logistieke keten begint binnen de eigen onderneming en security hoort een vast onderdeel met een eigen budget te zijn van de bedrijfsvoering. Het nemen van securitymaatregelen leidt wel degelijk tot kostenreductie en is een unique sellingpoint (USP). Security zorgt voor minder claims, het behoud van opdrachtgevers, maar ook voor nieuwe opdrachtgevers.

BEGIN MET RISICO ANALYSE

Zorg voor duidelijkheid naar opdrachtgevers en maak security bespreekbaar. Indien de logistiek dienstverlener richting verlader aangeeft dat het gevraagde beveiligingsniveau te laag is en dit niet wordt aangepast, leg dit dan schriftelijk vast. Het is dan aantoonbaar dat wel degelijk op de risico's is gewezen. Uiteraard is het altijd belangrijk om een gedegen afweging te maken of het verantwoord is om onder deze omstandigheden de opdracht aan te nemen. Door de bedrijfsprocessen, de risico's en de genomen maatregelen in kaart te brengen, ontstaat zicht op de risico's en de mate waarin die risico's zijn afgedekt.

Directe risico's:

- Inbraak, diefstal vanuit warehouse of vanaf bedrijfsterrein et cetera;
- Diefstal vanuit vrachtauto en overval op transporten in de openbare ruimte (weg, parkeerplaats, tankstation, bedrijventerrein et cetera);
- Faciliteren van diefstal, inbraak of overval door het lekken van informatie met betrekking tot goederen, data en route van transport, getroffen beveiligingsmaatregelen et cetera.



Training Security Awareness

Opdrachtgevers en klanten stellen steeds vaker de eis dat personeel van logistiek dienstverleners een training security-awareness heeft gevolgd. TLN biedt twee trainingen: Security Awareness en de AEO Security (Fenex). De trainingen hebben een laagdrempelige inhoud en incompanytrainingen zijn mogelijk. De training Security Awareness moet chauffeurs en warehousemedewerkers bewust maken van wat er allemaal in 'de grote boze buitenwereld' gebeurt. Chauffeurs leren hoe ze noodsituaties kunnen voorkomen en hoe zij kunnen handelen als ze toch in een noodsituatie belanden. De training telt mee voor 7 code 95-punten en is goedgekeurd voor SOOB-subsidie.

Tapa: aantoonbare beveiliging

Tapa (Transported Asset Protection Association) richt zich op beveiliging van de supplychain van diefstalgevoelige producten. Veel grote elektronikaverladers stellen aan vervoerders de eis om Tapa-gecertificeerd te zijn. Meer informatie via www.tapa-global.org. TLN Consultancy begeleidt het Tapa-certificeringstraject. Voor meer informatie: [mr. Hélène Minderman RSE, hminderman@tln.nl](mailto:mr.Hélène.Minderman@tln.nl).

dekmantel dienen voor onderwereld-organisaties, opererend in de bovenwereld.

UITBESTEED VERVOER

Doe altijd eerst onderzoek om vast te stellen met wie er precies zaken gedaan gaat worden. Dit is ook van toepassing bij het uitbesteden van vervoer via vrachttuitwisselingsplatformen. Er ontstaat een onaanvaardbaar risico bij de uitbesteding aan onbekende bedrijven. Check (bijvoorbeeld op Google Maps) of het bedrijf inderdaad op het opgegeven adres is gevestigd. Vraag naar het vaste telefoonnummer, check de website, vraag

naar referenties en een kopie van de verzekeringspolis (met sluitende dekking en bijbehorend betalingsbewijs). Raadpleeg ook het Centraal Insolventieregister, omdat het bedrijf intussen failliet kan zijn verklaard. Zie insolventies.rechtspraak.nl. Het is belangrijk om dit register erop na te slaan want vergunning, Kamer van Koophandel-inschrijving en verzekeringspapieren kunnen er goed uitzien, maar het is mogelijk dat ze niet in orde zijn. De lading wordt opgehaald door de nepvervoerder, maar komt nooit aan op het losadres. Het inschakelen van een charter ontslaat de ondernemer niet van zijn verantwoordelijkheid ten opzichte van zijn opdrachtgever. Belangrijk is ook de overeenkomst goed te lezen die de hoofdvervoerder heeft gesloten met zijn opdrachtgever.

BESCHERM DATA

Fysiek transport van goederen gaat altijd gepaard met datastromen die betrekking hebben op de goederen (aard, oorsprong en bestemming), het transport daarvan (modaliteit, data van vertrek en verwachte aankomst) en aanvullende gegevens op het gebied van douane of andere overheidsinstanties. Een bedrijf moet zelf kunnen aantonen, dat het voldoende 'in control' is met alle privacyregels. Er moet dus privacy- en beveiligingsbeleid zijn en dit moet vertaald worden in concrete maatregelen en procedures. Het is belangrijk dat ondernemers verwerkte persoonsgegevens goed beveiligen en zorgen dat alleen bevoegden bij de data kunnen.

Hélène Minderman is beleidsadviseur Strategie, Duurzaamheid en Bereikbaarheid bij TLN.

Achterliggende risico's:

- Onvoldoende gescreend personeel dat een crimineel verleden blijkt te hebben (werving- en selectierisico);
- Van oorsprong betrouwbaar personeel dat echter onvoldoende binding met zijn bedrijf heeft, zodat de stap naar criminaliteit of het faciliteren daarvan sneller wordt gemaakt (bedrijfscultuurrisico);
- Betrouwbaar personeel dat onvoldoende is getraind in het herkennen van risicosituaties en de daarvoor getroffen beveiligingsmaatregelen;
- Onvoldoende gescreende logistiek dienstverleners, die bijvoorbeeld als

SECURITY HOORT EEN VAST ONDERDEEL MET EEN EIGEN BUDGET TE ZIJN VAN DE BEDRIJFSVOERING