Where safety
& security
form a license
to operate

Your systems Integrator
for safety & security

Beveiligingslekken in de logistiek - risico's, trends en oplossingen

+32 3 653 08 38 - Mon-Fri: 7:30 - 16:00

info@rombitsolutions.com

Bredastraat 129, 2030 Antwerp, Belgium

Inhoudsopgave

Inleiding

De logistieke sector in Europa wordt geconfronteerd met toenemende beveiligingsrisico's. Criminelen richten zich steeds vaker op waardevolle goederen, waarbij ze gebruikmaken van geavanceerde methoden en profiteren van zwakke plekken in de supply chain. Deze whitepaper belicht de belangrijkste beveiligingslekken, onderbouwd met recente data en voorbeelden, en biedt oplossingen om deze risico's te mitigeren.

1. Fysieke beveiligingslekken

Onvoldoende perimeterbeveiliging

Wat houdt dit in?

De perimeterbeveiliging vormt de eerste verdedigingslinie van een logistieke site. Deze beveiliging bestaat doorgaans uit hekwerken, poorten, verlichting, cameratoezicht, slagbomen en sensoren. Als deze elementen ontbreken of onvoldoende functioneren, kunnen onbevoegden zich eenvoudig toegang verschaffen tot het terrein zonder direct opgemerkt te worden.

Belangrijkste risico's:

- Ongeautoriseerde betreding van het terrein zonder detectie
- Criminelen kunnen verkenning uitvoeren zonder verstoring
- Blind spots in camerabeelden laten kwetsbare zones onbeheerd
- Inbraak tijdens daluren (weekenden, nacht) zonder alarmdetectie
- Verlies van verzekeringsdekking bij ontoereikende fysieke maatregelen

Ondersteunende data en voorbeelden:

- In 2023 vond meer dan 60% van de diefstallen uit vrachtwagens plaats op locaties met onvoldoende omheining of verlichting (bron: TAPA EMEA Intelligence System).
- Uit een rapport van TT Club blijkt dat georganiseerde criminele netwerken vaak vooraf de perimeter scouten op kwetsbare plekken zoals slecht verlichte hoeken of defecte poorten.

Aanbevolen maatregelen:

- Installatie van dubbel hekwerk met detectie op fysieke manipulatie
- Slimme verlichting met bewegingssensoren, vooral in blinde hoeken
- Thermische camera's die beweging detecteren in het donker of bij mist
- Inzet van geautomatiseerde slagbomen en voertuigherkenning
- Centralisatie van camerabeelden in een meldkamer met live monitoring

Gebrekkige toegangscontrole

Wat houdt dit in?

Toegangscontrole omvat de verificatie, registratie en monitoring van personen en voertuigen die het terrein betreden. Dit geldt voor vaste medewerkers, tijdelijke krachten, leveranciers, chauffeurs en bezoekers. Een gebrek aan gecontroleerde toegang vergroot de kans op interne fraude, diefstal en veiligheidsinbreuken.

Belangrijkste risico's:

- Personen kunnen zich als legitieme bezoeker voordoen (social engineering)
- Gebruik van gedeelde of ongecontroleerde toegangspassen
- Geen overzicht wie zich op welk moment waar bevindt
- Gebrek aan historische logdata bemoeilijkt onderzoek bij incidenten
- Voertuigen kunnen meeliften via open slagbomen zonder verificatie

Relevante cijfers:

- In 2022 werd bij 26% van alle gerapporteerde ladingdiefstallen in Europa interne betrokkenheid vastgesteld (bron: Munich Re).
- Slechts 34% van Europese logistieke bedrijven maakt gebruik van elektronische toegangsregistratie met logfunctionaliteit (bron: EU Security Tech & Logistics Report 2023).
- In veel gevallen gebeurt toegang nog steeds met papieren bezoekerslijsten of losse sleutels, die makkelijk te dupliceren zijn.

Aanbevolen maatregelen:

- Gebruik van biometrische toegangscontrole (vingerafdruk, gezichtsherkenning) voor gevoelige zones zoals serverruimtes, magazijnen en laadstations
- Digitale tijdsregistratie gekoppeld aan toegangspoorten
- Unieke QR- of NFC-badges gekoppeld aan identiteitsverificatie
- Realtime notificaties bij afwijkend gedrag, zoals toegang buiten werktijden
- Gebruik van anti-passback en zonescheiding om meeliften of doorschuiven te voorkomen
- Implementatie van contractor management software om externe partijen vooraf te registreren en monitoren

2. Transportgerelateerde risico’s

Fictieve ophaalmomenten (impersonatie van transporteurs)

Wat houdt dit in?

Bij een fictief ophaalmoment doen criminelen zich voor als een gecontracteerde of verwachte chauffeur of vervoerder. Ze gebruiken valse documenten, vermommingen of zelfs gekopieerde bedrijfskleding en vrachtwagens om overtuigend over te komen. Vervolgens vertrekken ze met waardevolle lading zonder dat er sprake is van geweld of inbraak – het is logistieke fraude in zijn meest geraffineerde vorm.

Belangrijkste risico’s:

- Goederen verdwijnen zonder sporen van geweld of forcering
- Vertraging in ontdekking van het incident, wat traceerbaarheid bemoeilijkt
- Verminderde klantvertrouwen en juridische aansprakelijkheidsdiscussies
- Exploiteerbare zwakheden in planningssoftware of dispatch-protocollen

Ondersteunende data:

- In 2023 registreerde TAPA EMEA een toename van 45% in impersonatie-incidenten bij ladingafhalingen, vooral in West-Europa.
- TT Club en BSI schatten dat 10–12% van alle supply chain diefstallen wereldwijd een vorm van impersonatie betreft.

Aanbevolen maatregelen:

- Gebruik van digitale verificatiesystemen waarbij transportopdrachten gekoppeld zijn aan unieke voertuig- en chauffeur-ID’s
- Cross-check van identiteitsdocumenten, kenteken en transportopdracht via centrale dispatch-software
- Verificatie van externe transporteurs via QR-code of token-gebaseerde check-in
- Bodycams of geofencing voor ‘dock verification’ bij gevoelige lading
- Train personeel op het herkennen van vervalste documenten en afwijkende gedragingen
-

Slash-and-grab diefstallen

Wat houdt dit in?

Bij een slash-and-grab-aanval snijden criminelen tijdens een korte stilstand, vaak ‘s nachts of op parkeerplaatsen, het zeildoek van een vrachtwagen open om snel waardevolle lading eruit te halen. Ze werken in groepen en nemen alleen gemakkelijk verhandelbare producten mee, zoals elektronica, cosmetica of sigaretten.

Belangrijkste risico's:

- Goederen verdwijnen zonder sporen van geweld of forcering
- Fysieke schade aan voertuig en lading
- Onverzekerde verliezen bij onvoldoende beveiliging of parkeervoorschriften
- Verlies van klantrelaties door vertragingen of ontbrekende leveringen
- Georganiseerde bendes met snelle vluchtauto's bemoeilijken opsporing

Cijfers en trends:

- In 2023 vond meer dan 60% van alle slash-and-grab diefstallen in Europa plaats in Duitsland, gevolgd door Frankrijk en Nederland.
- Volgens het BSI Supply Chain Intelligence Report is dit type diefstal goed voor ongeveer 20% van alle geregistreerde vrachtcriminaliteit in Europa.
- De gemiddelde schade per incident wordt geschat op €30.000 tot €80.000, exclusief gevolgschade.

Voorwaarden die het risico verhogen:

- Parkeren op onbeveiligde of slecht verlichte rustplaatsen
- Gebrek aan fysieke barrières (zoals ladingdragers aan de binnenkant van het zeildoek)
- Geen alarm- of detectiesystemen bij stilstand
- Geen gebruik van beveiligde parkeerplaatsen (TAPA PSR-gecertificeerd)

Aanbevolen maatregelen:

- Gebruik van versterkte of snijbestendige zeilen met stalen draadinleg
- Alarm- en GPS-systemen die waarschuwen bij ongeautoriseerde opening
- Parkeren op TAPA PSR-gecertificeerde locaties
- Vermijden van stilstand in risicovolle gebieden (bekend bij politie en TAPA)
- Chauffeursvoorlichting over nachtelijke risico's en gedragsprotocollen bij incidenten

3. Interne bedreigingen

Wat houdt dit in?

Interne bedreigingen binnen de logistieke keten verwijzen naar diefstal, sabotage of lekken van informatie door medewerkers, ingehuurde krachten, onderaannemers of andere personen met legitieme toegang tot goederen en systemen. In tegenstelling tot externe inbraken zijn deze incidenten moeilijker te detecteren, omdat daders vaak bekend zijn met de processen en zwakke plekken binnen het bedrijf.

Belangrijkste risico's:

- **Diefstal van lading of materialen** door personeel met magazijntoegang
- **Manipulatie van digitale systemen** zoals planningssoftware, scanningsapps of ERP
- **Lekken van vertrouwelijke informatie**, zoals klantgegevens, leveringsschema's of toegangscodes
- **Sabotage van leveringen of infrastructuur**, al dan niet uit wraak of onder druk van georganiseerde netwerken
- **Faciliteren van externe inbraken** door het delen van routes, openingsschema's of beveiligingscodes

Ondersteunende data:

- In 2022 werd bij 26% van alle ladingdiefstallen in Europa vastgesteld dat er interne betrokkenheid was. Dat blijkt uit gegevens van Munich Re, gebaseerd op politieverslagen, verzekeringsclaims en TAPA-rapportages.
- Volgens een studie van BSI en TT Club wordt tot 35% van alle logistieke fraude wereldwijd mogelijk gefaciliteerd door interne actoren.
- Supply chain organisaties geven in een ENISA-rapport (European Union Agency for Cybersecurity) aan dat interne bedreigingen in de top 3 staan van grootste beveiligingszorgen.

Waarom zijn interne bedreigingen zo gevaarlijk?:

- **Hoge mate van vertrouwen:** Interne medewerkers hebben vaak onbeperkte toegang tot kritieke zones zonder directe controle.
- **Moeilijk detecteerbaar:** Incidenten kunnen lang onopgemerkt blijven zonder logregistratie of videobewijs.
- **Social engineering en chantage:** Medewerkers kunnen onder druk of tegen betaling informatie doorspelen aan criminele netwerken.
- **Verhoogde risico's bij tijdelijke krachten en onderaannemers**, waarvoor vaak minder strenge screening geldt.

4. Cybersecurity kwetsbaarheden

Wat houdt dit in?

De snelle digitalisering van de logistieke sector heeft geleid tot een sterke toename in het gebruik van softwareplatforms, IoT-apparaten, telematica, API-koppelingen en cloudgebaseerde systemen. Deze technologieën verhogen de efficiëntie, maar openen ook nieuwe aanvalsvectoren voor cybercriminelen. Kwetsbaarheden ontstaan wanneer deze systemen onvoldoende beveiligd, slecht onderhouden of niet goed geïntegreerd zijn.

Belangrijkste risico's:

- **Ransomware-aanvallen** die hele magazijnen of transportplanningen stilleggen
- **Datalekken** van klantinformatie, leveringsdata, prijslijsten of transportcontracten
- **Manipulatie van routes, voorraadniveaus of orderdata** via gekraakte systemen
- **Toegang tot camera's of toegangscontrole via onbeveiligde IoT-apparaten**
- **Phishing en social engineering** gericht op logistieke medewerkers of dispatchers

Kwetsbare punten in de logistieke IT-keten:

1. **Verouderde software** zonder recente beveiligingspatches
2. **Gebrekkige wachtwoordbeveiliging** (zoals hergebruik of ongewijzigde standaardinstellingen)
3. **IoT-apparaten zonder firmware-updates** (zoals slimme camera's, sensoren, GPS-tracking units)
4. **Onveilige externe verbindingen** via leveranciers, onderaannemers of klantportals
5. **Geen of gebrekkige netwerksegmentatie** tussen kantoor- en operationele systemen (OT/IT)

5. Onveilige parkeerplaatsen

Wat houdt dit in?

Vrachtwagenchauffeurs zijn wettelijk verplicht om rustpauzes te nemen tijdens hun ritten, vaak langs autosnelwegen of in de buurt van distributiecentra. Deze rustmomenten vormen een cruciaal moment voor criminele groepen om toe te slaan, zeker wanneer er geen gebruik wordt gemaakt van beveiligde parkeerterreinen.
Veel van deze openbare of informele parkings zijn slecht verlicht, onvoldoende bewaakt en hebben geen gecontroleerde toegang. Criminelen weten dit en richten zich actief op deze locaties om goederen te stelen of voertuigen open te breken. Vooral nachtelijke stops zijn kwetsbaar.

Belangrijkste risico's:

- **Slash-and-grab diefstallen:** Zeilen van trailers worden doorgesneden om snel goederen te pakken zonder het alarm te activeren.
- **Georganiseerde bendeactiviteit:** Voertuigen worden systematisch gevolgd tot ze op een onbeschermde parkeerplek stilstaan.
- **Fictieve 'hulpverlening':** Criminelen doen zich voor als medewerkers van de parkeerlocatie of technische dienst om toegang tot de lading te verkrijgen.
- **Ladingdiefstal zonder inbraak:** Gebruik van 'keyless' relays of gekopieerde sleutels bij slecht bewaakte truckstops.

Ondersteunende data:

- Volgens TAPA EMEA is het gebrek aan beveiligde parkeerplaatsen een van de grootste structurele veiligheidsproblemen in Europa. Er is momenteel een tekort van **meer dan 400.000 beveiligde truckparkings**.
- In meer dan **50% van alle ladingdiefstallen** in Europa vindt het incident plaats wanneer het voertuig geparkeerd staat, vaak tijdens verplichte rusttijden (Bron: TAPA EMEA Intelligence System).
- Een studie van IRU (International Road Transport Union) toonde aan dat **meer dan 75% van de Europese chauffeurs zich onveilig voelt** tijdens rustpauzes vanwege slechte parkeerfaciliteiten.

Waarom zijn deze situaties extra risicovol?

- Chauffeurs bevinden zich vaak alleen en hebben weinig verdedigingsmogelijkheden
- Parkeerplaatsen zijn zelden uitgerust met cameratoezicht, slagbomen of controlepersoneel
- Vrachtwagens met herkenbare merklogo's of douanezegels trekken extra aandacht
- Geen directe meldingssystemen of hulpdiensten in de buurt bij incidenten

Aanbevolen maatregelen:

Beveiligingsmaatregelen voor vervoerders:

- Gebruik van **TAPA PSR-gecertificeerde** parkeerplaatsen met slagbomen, CCTV, omheining en bemande toegang
- **Slimme beveiliging op voertuigniveau**, zoals GPS-geofencing, bewegingssensoren in trailers en automatische vergrendeling van deuren bij stilstand
- **Afschermende ladinghoezen** zonder logo's of productindicatie
- Vooraf geplande ruststops op beveiligde locaties, geïntegreerd in de routeplanning

Beleidsmaatregelen voor bedrijven en beleidsmakers:

- Samenwerking met overheid en politie voor de aanleg en certificering van beveiligde truckparkings
- Inzet van Europese fondsen voor uitbreiding van beveiligde parkeerinfrastructuur
- Real-time datadeling tussen logistieke bedrijven over verdachte parkeerlocaties

Chauffeurstraining en bewustwording:

- Instructies over risicogedrag: bijvoorbeeld niet parkeren op verlaten of slecht verlichte plekken
- Uitgerust zijn met meldingsapparatuur, panic buttons en communicatietools
- Bewustzijn creëren over signalen van surveillance of 'volging' door verdachte voertuigen

Conclusie

De beveiliging van logistieke ketens in Europa staat onder toenemende druk. De cijfers zijn alarmerend: georganiseerde criminaliteit wordt professioneler, interne bedreigingen worden geraffineerder, en digitale kwetsbaarheden groeien mee met de snelheid van digitalisering. Tegelijkertijd blijven fysieke beveiligingslekken – zoals gebrekkige perimeterbeveiliging, falende toegangscontrole en onveilige parkeerplaatsen – onverminderd bijdragen aan de toename van incidenten.

De logistieke sector moet daarom de stap zetten van reactief naar proactief risicobeheer. Dat betekent:

- investeren in geïntegreerde fysieke en digitale beveiligingsoplossingen;
- inzetten op mensgerichte maatregelen zoals screening, opleiding en awareness;
- en gebruikmaken van internationale standaarden zoals **TAPA FSR, TSR en PSR** om aantoonbaar veilig te opereren.

Bedrijven die beveiliging als strategische prioriteit behandelen, winnen niet alleen aan veiligheid, maar ook aan operationele stabiliteit, klantvertrouwen en concurrentievermogen. Beveiliging is geen kostenpost, maar een waardevolle investering in bedrijfscontinuïteit.

Wil jij jouw logistieke operaties beter beschermen tegen interne én externe bedreigingen?

✅ Laat je supply chain doorlichten op beveiligingslekken
✅ Ontvang advies over TAPA-compliance en slimme technologie-integraties
✅ Bouw aan een risicobewust veiligheidsbeleid dat werkt – voor én met je mensen

👉 **Plan nu een vrijblijvende beveiligingsscan met onze experts**

Of neem rechtstreeks contact op voor een demo van onze geïntegreerde securityoplossingen. Samen maken we jouw logistiek veiliger, slimmer en toekomstbestendig.