

TAPA EMEA
Transported Asset Protection Association

TAPA EMEA Driver Security Guide

TAPA EMEA Copyright © Do Not Copy



SWEDISH

Innehållsförteckning

INTRODUKTION OCH SÄKERHETSMILJÖ FÖR LEVERANSKEDJAN	3
KOMMUNIKATION MED POLIS OCH LEDNING.....	4
TYPER AV KRIMINELL AKTIVITET	5
INTRÅNG, RÅN OCH STÖLD.....	6
BEDRÄGERI.....	8
KAPNING.....	11
ILLEGAL INVANDRINGSINTRÄDE	13
BROTTLIGHET MOT SISTA MILENS FORDON	15
CYBERBROTT OCH LÄCKA AV INFORMATIONSSÄKERHET	17
DISPATCH- ELLER ÖVERVAKNINGS- OCH RESPONSCENTERS FUNKTIONER OCH STÖD TILL FÖRARE	19
EUROPEISKA NÖDNUMMER.....	21
VIKTIGA REGLER FÖR FÖRARE.....	22
REFERENCES.....	23

Introduktion och säkerhetsmiljö för leveranskedjan

Laststöld är ett betydande problem globalt sett. Största delen av frakttransporten i Europa sker på väg. Likaså i övriga länder i Europa, Mellanöstern och Afrika. Speciellt för Europeiska unionen kan laststöld på väg betraktas som ett hot mot en av EU kärnprinciper, den fria rörligheten för varor. Årliga förluster till följd av laststöld i Europa uppskattas till 8,2 miljarder euro eller en genomsnittlig värde på 6,72 euro per resa.

- Endast under 2023 rapporterades över 50 000 laststölder till TAPA EMEA, vilket motsvarar över 140 stölder per dag.
- Under de senaste tre åren har genomsnittsförlusten för rapporterade större brott med ett värde över 100 000 euro varit över en miljon euro.
- Under samma period är värdet på stulna varor från leveranskedjor i EMEA-regionen varje 24 timmar något över 800 000 euro.
- I Sydafrika har det skett en liten minskning av registrerade lastbilstillslag, men en ökning av rån mot kontanttransporter.
- Av dessa lastbilsbrott:
 - I genomsnitt är 80% stölder från lastbilar/lastbilsflak.
 - Av de 80%, sker 10% på icke-säkra parkeringsplatser.

"Både opportunistiska och organiserade attacker är sannolika under lasttransport på väg. När det gäller opportunistiska hot är frånvaron av 'möjlighetsgivande' nyckeln till att minska dessa incidenter. Å andra sidan är det avgörande att förstå kriminella nätverks modus operandi för att effektivt kunna hantera kriminalitet relaterad till lasttransport. Dessa kriminella nätverk verkar över gränserna och använder ofta lagliga affärsstrukturer för sina aktiviteter. Sektorer som konstruktion, hotell och logistik är särskilt sårbara för infiltration av organiserad brottslighet.



Kommunikation med polis och ledning

Effektiv kommunikation med polis och transportföretagens ledning är avgörande för förare, särskilt under ovanliga situationer. I dessa olyckliga situationer måste förare kommunicera viktig information på ett tydligt och korrekt sätt. Språkbarriärer kan utgöra en utmaning, eftersom förare kanske inte talar det lokala språket. I sådana fall finns det mekanismer som tillhandahålls av professionella övervakningscentraler som kan hjälpa genom att använda infödda talare för att kommunicera med lokala myndigheter. Vissa av dessa övervakningscentraler har ett nätverk av centraler och säkerhetsföretag längs förarnas rutter för att ge stöd vid händelser, antingen genom att tillhandahålla säkerhetstjänster på plats om det behövs eller för att underlätta lokal interaktion med polis och medicinska akutsjukvårdstjänster.

Vid en säkerhetsincident måste förarna kunna kommunicera följande information korrekt med polisen:

- Förarens namn och registreringsnummer för fordonet (lastbil och släpvagn)
- Speciella egenskaper hos fordonet (färg, märke, speciella logotyper etc.) som ska underlätta för polisstyrkorna att lokalisera fordonen
- Fordonets plats (så exakt som möjligt) med hjälp av antingen km-markering på vägen, eller närmaste stad/by passerad, eller någon landmärke (t.ex. servicestation etc.).

- Typ av incident och om medicinsk support behövs.

Kommunikation med transportföretagens ledning vid en incident bör ge samma noggrannhet och en minsta uppsättning information, fokuserad främst på de två sista punkterna ovan, eftersom förarnas och fordonens data är välkända för transportföretagen..



Typer av kriminell aktivitet

I denna Säkerhetsguide för Förare kommer vi att utforska vanliga typer av kriminella aktiviteter och ge tips om förebyggande, respons och rapportering. Enligt den senaste Europol-rapporten finns det 821 kriminella nätverk i EU med över 25 000 medlemmar. Dessa nätverk ägnar sig åt olika brott, inklusive narkotikahandel, bedrägeri, egendomsbrott, människosmuggling och människohandel. Narkotikahandel är en framträdande aktivitet, där 50% av de mest hotande kriminella nätverken är involverade, och 36% enbart fokuserade på narkotikahandel. Vi kommer också att analysera flera specifika typer av kriminell verksamhet på ett sätt som presenterar endast de ämnen som direkt kan påverka förarna och ge vägledning med enkla åtgärder som förarna måste vidta eller undvika under sådana händelser. I de flesta av de analyserade brottskategorierna har vi också inkluderat några relaterade exempel.

MOST TARGETED PRODUCTS – TOP 5 COUNTRIES



South Africa

1. Phones
2. Cash
3. Misc. Electronics
4. Metal
5. Food & Drink



United Kingdom

1. Fuel
2. Food & Drink
3. Tobacco
4. Clothing & Footwear
5. No Load (Theft of truck and/or trailer)



Germany

1. Fuel
2. Metal
3. Tools/Building Materials
4. Auto Parts
5. No Load (Theft of truck and/or trailer)



France

1. Fuel
2. Metal
3. Jewellery/Precious Metals
4. Misc. Electronics
5. Food & Drink



Sweden

1. Fuel
2. Metal
3. No Load (Theft of truck and/or trailer)
4. Cash
5. Food & Drink

Note: TAPA EMEA is recording losses in over 20 TIS product categories. However, across EMEA, most recorded cargo crimes stated the products targeted as unspecified or miscellaneous.

Intrång, Rån och Stöld

Vad är hotet om intrång, rån och (last-/bränsle) stöld?

Det finns flera situationer där brottslingar lyckas ta sig in i lastutrymmet (intrång) och delvis stjäla last från det. Det finns också fall där brottslingar lyckas stjäla hela lastbilar eller släpvagnar med full last.

Hur man förebygger hotet om intrång, rån och stöld?

För att minska risken för intrång, rån eller stöld är det klokt att hålla sig till den planerade rutten och undvika oplanerade stopp eller ändringar, eftersom dessa oplanerade händelser erbjuder brottslingarna den önskade möjligheten att attackera. Även om att följa planen inte garanterar fullständig säkerhet och trygghet minskar det betydligt risken för att bli offer.

Vidare rekommenderas det att inte anlända för tidigt till destinationsanläggningen, eftersom väntan utanför exponerar både föraren och lasten för brottslingar som är aktiva på logistikområden.

Dessutom har det nyligen skett en anmärkningsvärd ökning av rapporterade incidenter med bränslestöld, som involverar både små och stora mängder diesel.

Om du redan har påverkats eller blivit ett offer för en incident/rån, vänligen dela typen, omfattningen, platsen och vilken typ av produkter som var involverade med oss genom följande e-postadress: tisteam@tapaemea.org. På så sätt kan vi registrera incidenten i vår TAPA EMEA-databas och hjälpa andra förare och disponenter att reagera på relevanta trender

THEFT FROM VEHICLE INCIDENT ON 12.03.2024

Incident Details	Place	Product
DATE 12.03.2024	City -	CATEGORY Miscellaneous Electronics
INCIDENT CATEGORY Theft from Vehicle	REGION/ COUNTRY -/ Germany	PRODUCT DETAILS Electrical appliances
MODUS OPERANDI Intrusion	LOCATION TYPE Unclassified Parking	VALUE IN EUR 150,000.00
	LATITUDE/ LONGITUDE 51.401352397921/ 11.719513675255	

Source: TIS database

THEFT FROM TRAILER INCIDENT IN 20.02.2024

Incident Details	Place	Product
DATE 20.02.2024	City Naples	CATEGORY Miscellaneous
INCIDENT CATEGORY Theft from Vehicle	REGION/ COUNTRY -/ Italy	PRODUCT DETAILS Perfumery and Tobacco products
MODUS OPERANDI Intrusion	LOCATION TYPE Unclassified Parking	VALUE IN EUR 2,400,000.00
	LATITUDE/ LONGITUDE 40.8517746/15.2681244	

Source: TIS database

Säkra parkeringsområden

När du tar pauser under din rutt rekommenderas det att använda säkra parkeringsområden. Rådfråga dina disponenter innan du påbörjar din resa för att lokalisera dessa säkra parkeringsområden längs din rutt.

Fördelarna med att använda säkra parkeringsområden inkluderar:

- Förbättrad säkerhet för både föraren och lasten, vilket minskar risken för kriminell aktivitet.
- Tillgång till vilorum och hygienfaciliteter för att hjälpa förare att koppla av under sina pauser.
- I händelse av en incident kan säkerhetssystem som övervakningskameror (CCTV) ge bevis för att stödja polis- och interna utredningar.

Oplanerade stopp och oväntade ändringar av rutter

Brottslingar söker ofta utnyttja eventuella oregelbundenheter i din rutt, eftersom de ser dem som möjligheter att attackera dig och stjäla lasten. Det är avgörande att förbli vaksam och minimera eventuella oplanerade avvikelser eller störningar som kan skapa sådana möjligheter.

Hur man svarar på hot om intrång, rån och stöld?

Gör







- Skydda dig själv. Om du är i din hytt, stanna där inne.
- Ring omedelbart polisen.
- Om din lastbil är utrustad med en panikknapp, tryck på den, eller försök kommunicera med ditt övervaknings-/dispositionscenter.
- Samla så mycket information från brottslingarna som möjligt för att dela med polisen.
- Bevara brottsplatsen för att stödja utredningsteamet.
- Om du måste parkera utanför ett säkert parkeringsområde:
 - o Positionera lastdörrarna på din lastbil/släpvagn mot en vägg, byggnad eller annan lastbil/fordon.
 - o Håll stoppet/pausen så kort som möjligt.
- Använd låsbara bränslelock och antisifonanordningar för att förhindra bränslestöld.

Undvik

- FÖRSÖK INTE att försvara lasten genom att konfrontera brottslingarna, eftersom det kan sätta ditt liv i fara.
- ÄNDRA INTE din planerade resväg och schemalagda stopp om det inte är nödvändigt, och informera ditt dispositionscenter samtidigt som du vidtar extra säkerhetsåtgärder.
- ÄNDRA INTE din leveransadress utan positiv bekräftelse från din disponent.
- LITA INTE på förbipasserande för att guida dig om du är vilse; det är bättre att fråga dem om information om din plats istället.

Hur man rapporterar hot om intrång, rån och stöld?

Om du upplever en säkerhetsincident som involverar intrång som resulterar i rån eller stöld av din last, rapportera enligt nedan eller rapportera följande information till polisen/övervakningscentret och/eller dispositionscentret:

-  Tid/datum/plats för incidenten
-  Eventuella skador eller behov av akut sjukvård
-  Förarens namn / registrerings skylt för lastbil/släpvagn
-  Antal inblandade brottslingar
-  Brottslingarnas tillvägagångssätt (hur det hände)
-  Beräknad lastförlust

Bedrägeri

Vad är bedrägerihot?

I många fall kommer angripare att försöka få tillgång till lasten inte genom att angripa den med våld utan genom sidospår. Detta tillvägagångssätt innebär att använda bedrägliga medel för att lura mäklare, transportörer, avsändare och naturligtvis förare att överlämna lasten till tjuvarna istället för ett legitimt företag. Tjuvar kommer att utge sig för att vara legitima avsändare, mäklare, polis eller andra myndigheter, till och med förare, för att få lasten. I vissa fall kan angripare rikta in sig på säkerhetssystemen ombord på fordonen och försöka förvirra eller vilseleda föraren om lastens plats. De kan också avlyssna eller blockera kommunikationen mellan föraren, avsändnings-/övervakningscentralen eller polismyndigheterna. Att avlyssna fordonsensorer och enheter är en annan taktik som används av angripare mot lasttransporter.

Falska förarhämtningar utgör cirka 2 % av de totala laststöldrarna i Europa, men i vissa fall är förlusterna av betydande värde. I november 2023 lyckades en falsk förare som utgav sig för att vara den riktiga stjäla mobiltelefoner från Schiphols flygplats i Amsterdam, till ett värde av mer än 1,5 miljoner euro.

THEFT OF TRAILER INCIDENT ON 10.11.2023

Incident Details	Place	Product
DATE 10.11.2023	City Reims	CATEGORY Food & Drink
INCIDENT CATEGORY Theft of Trailer	REGION/COUNTRY -/France	PRODUCT DETAILS champagne
MODUS OPERANDI Deception Others	LOCATION TYPE En Route	VALUE IN EUR 600,000.00
	LATITUDE/ LONGITUDE 49.258329/ 4.031696	

Source: TIS database

Hur man förebygger bedrägerihot?

- **Förhindra utklädnad**
För att förhindra utklädnad och potentiella bedrägliga handlingar från kriminella är det viktigt att vara försiktig och följa dessa riktlinjer:
 - Om du blir stoppad av någon som utger sig för att vara polis eller annan myndighet för en kontroll, var vaksam och överväg möjligheten att det är en förklädnad.
 - Om en anställd på lagret strax innan ankomst till leveransfaciliteten informerar dig om att du måste leverera till en annan plats, verifiera alltid informationen med din avsändningscentral innan du fortsätter.
- **Undvik störning och falsksignalering**
Störning innebär att avsiktligt blockera kommunikationssignaler, vilket gör att enheter inte kan sända eller ta emot någon form av kommunikation (röstsamtal, SMS, larmsignaler, etc.). Falsksignalering, å andra sidan, innebär att bedragare använder bedrägliga tekniker för att vinna offrens förtroende genom att ändra uppringar-ID eller skicka meddelanden som verkar komma från en annan källa, vilket förare anser vara pålitligt.

On 16 May 2023, cargo thieves attacked and hijacked a truck travelling en route from Port Elizabeth to Cape Town, South Africa. The truck driver was shot and seriously injured.

After taking control of the vehicle, the offenders used a GPS jammer to delay security monitoring services and drove the vehicle to a remote location to offload and steal its cargo.

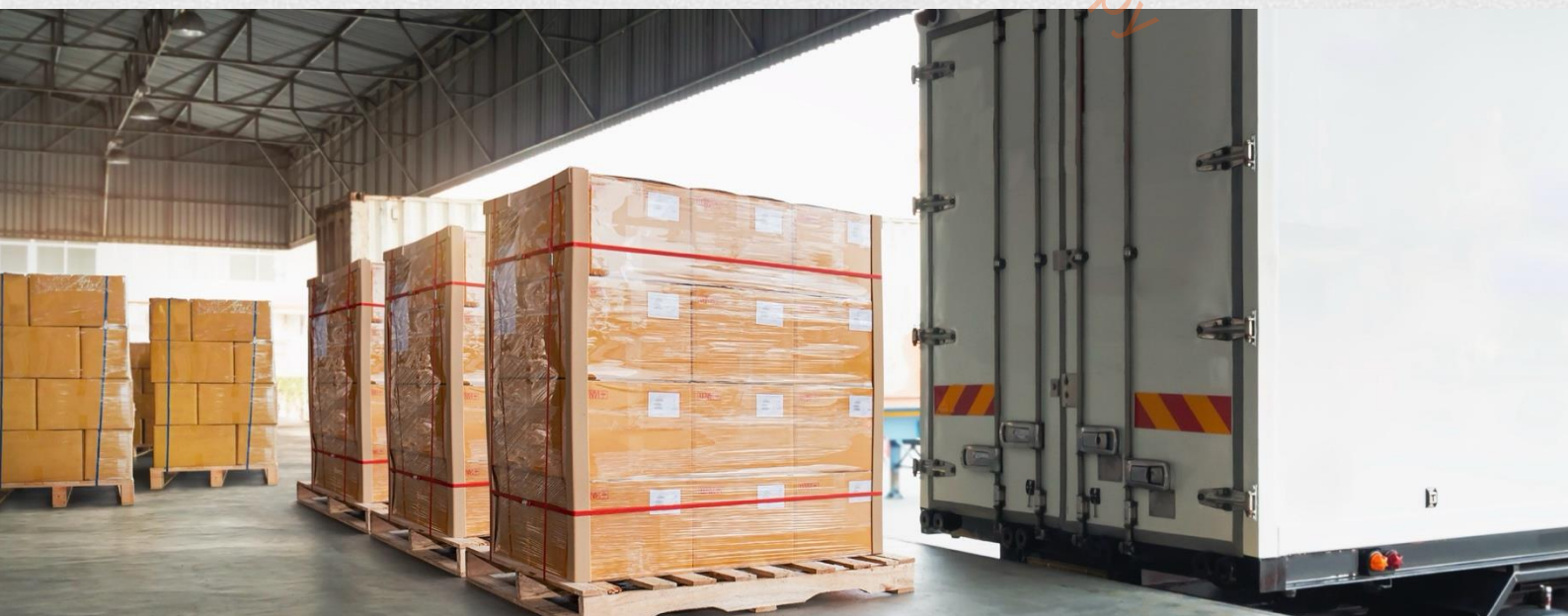
The target: catalytic converters.

This is just the latest in a series of high value and violent attacks on automotive supply chains in the Europe, Middle East & Africa (EMEA) region, with catalytic converters the prime target. In the last 18 months, thefts of catalytic converters have been reported to the TAPA EMEA Intelligence System (TIS) in France, Germany, and the United Kingdom as well as in South Africa. While most crime reports stating this product type do not share financial loss data, these are known to be significant, high value incidents.

Yet, as with so many other types of cargo crime, the number of recorded thefts is believed to represent only a small minority of the total number of incidents taking place.

Falsksignalering används ofta för att lura offer att avslöja känslig data eller för att genomföra lösenförhandlingar samtidigt som angriparens identitet döljs. Kriminella nätverk kan till och med erbjuda falsksigntjänster till andra brottslingar.

Inom lasttransport använder kriminella ofta GPS-falsksignalering för att manipulera den visade platsen på förarens enhet, vilket leder dem bort från sin avsedda rutt och gör dem sårbara för attacker.



- **Stöld från Rörliga Fordon (intern och extern)**

Det var tio år sedan Europol varnade för ett nytt fenomen där brottslingar använder sig av en 'Trojansk häst'-metod för att få tillgång till leveranslastbilar genom att gömma sig i stora träboxar. Boxarna, märkta som 'Fragile', hämtas av pakettjänster. När boxen är inne i lastbilen, på väg till sin slutdestination, smiter brottslingarna ut från boxen för att stjäla värdefulla föremål också inne i lastbilen, såsom smycken, telefoner eller elektronik. Medhjälpare som följer på avstånd simulerar sedan en olycka för att stoppa fordonet, vilket gör att de gömda kan fly genom hål som skurits ut i fordonets tak.

Stölder av gods med simulerade olyckor är ganska vanliga och stölder från rörliga lastbilar har också rapporterats regelbundet. Dock var den ovan beskrivna 'Trojansk häst'-modus operandi vid den tiden ett nytt fenomen.

En annan intressant modus operandi är den där brottslingar följer den rörliga lastbilen i samma hastighet. De positionerar sig i lastbilens döda vinkel, vanligtvis bakom, där lastbilsföraren inte kan se dem i speglarna. Sedan klättrar de upp på släpvagnen, bryter sig in i lastbilens last och går ombord på fordonet för att genomföra stölden. Medhjälpare följer med på ett fast mycket litet avstånd bakom den attackerade lastbilen för att ta emot de stulna varorna. Vid attackens slut återvänder de ombordvarande till hemfordonet och saktar ner för att komma ifrån lastbilen.

Hur man svarar på ett bedrägerihot?

Gör




- Om du misstänker att polisen eller andra myndigheter som stoppar dig längs din rutt inte är legitima:
 - Ring polisen för att bekräfta stoppets legitimitet och informera dem om dina farhågor.
 - Informera alltid din dispatching-/övervakningscentral om tecken från myndigheterna på vägen som uppmanar dig att stanna ditt fordon.
 - Be myndigheterna att följa med dig till närmaste polisstation för nödvändiga kontroller samtidigt som du håller din dispatching-/övervakningscentral informerad.
- Installera ett högsäkerhetslås för att undvika att lastutrymmets dörrar öppnas under körning.
- Installera sensorer som informerar dig när baddörrarna är öppna under färd.

Undvik

- FÖRLITA DIG INTE blindt på individer som påstår sig vara polis eller andra myndigheter utan att verifiera deras legitimation eller identifikation.
- AVVIK INTE från din planerade rutt eller ändra leveransplatser utan att bekräfta med ditt avsändnings- / övervakningscenter.
- TVEKA INTE att rapportera misstänkta incidenter eller bekymmer till polisen, ditt avsändnings- / övervakningscenter och relevanta myndigheter.

Hur rapporterar man ett Bedrägerihot?

Om du stoppas av polis eller andra myndigheter för kontroller, kontakta omedelbart ditt avsändnings- eller övervakningscenter och ge information om:

-  Din plats.
-  Typ av myndigheter (om möjligt).
-  Någon fordonets registrerings skylt eller andra kännetecken på myndigheterna.

Kapning

Vad är kapningshot?

Kapning innebär att stjäla (last) från en lastbil eller annat fordon efter att ha tvingat det att stanna, dvs. att kapa en last tobak. Det innebär också att råna ett fordon efter att ha tvingat det att stanna, ofta istället för våld. Kapningsincidenter utgör en betydande risk för förare, med potential för allvarliga skador eller till och med dödsfall.



Thorsten Neumann highlighted three extreme contributors to the data presented for the first three-quarters of the year. These included €300 million of losses recorded in just two crimes; one involving the hijacking of miscellaneous goods in Belgium, and the other a case of fraud detected within a metal supply chain by a global organisation based in Germany.

Hur förhindrar man kapningshot?

- **Var uppmärksam under körningen**
Som i definitionen, i kapningssituationer måste lastbilen stanna för att brottslingarna ska kunna ta kontroll över den, därför är det viktigaste sättet att undvika kapningssituationer att inte stanna när dessa situationer är uppenbara och omedelbara. Till exempel, om individer som inte verkar vara legitima myndigheter ber dig att stanna på vägen, är det viktigt att vara försiktig och prioritera din säkerhet. Även individer som utger sig för att vara falska poliser eller andra myndigheter kan utgöra en risk.
- **Identifiering av nya hot**
Det är avgörande att vara vaksam och förberedd för att hantera fientliga situationer. Vanligtvis följer kapare dig antingen innan de försöker ta kontroll över fordonet eller kör framför dig i konstant hastighet för att övervaka ditt körbeteende.

Hur man reagerar på kapningshot?

Gör







- Håll alla dörrar och fönster låsta under körning.
- Var vaken och medveten om din omgivning. Observera eventuella misstänkta eller ovanliga aktiviteter, fordon eller individer.
- Försök att skapa avstånd mellan ditt fordon och det misstänkta fordonet, så att om de stoppar dig kan du göra en manöver och köra iväg.
- Bibehåll regelbunden kontakt med ditt avsändnings-/övervakningscenter eller andra angivna kontakter och dela med dig av uppdateringar om din plats och eventuella avvikelser från den planerade rutten.

Undvik

- LÅT INTE någon person åka i din hytt.
- STOPPA INTE och kliv ur fordonet om du inte har bekräftat legitimiteten hos myndigheter som begär det.
- MOTSTÅ INTE eller konfrontera kaparna.
- GÖR INTE plötsliga eller misstänkta rörelser.
- GE INTE onödigt information till kaparna

Hur man rapporterar kapningshot?

Efter en kapning är det avgörande att rapportera händelsen till polisen och ditt avsändnings-/övervakningscenter så snart det är säkert att göra det. Ge dem alla relevanta detaljer för att underlätta utredningen:

-  Tid/datum/plats för händelsen och din nuvarande plats (om annorlunda än händelsens plats).
-  Eventuella skador eller behov av akut hälsovård.
-  Förarens namn/fordonets registrerings skyltar för lastbil/släpvagn.
-  Antal brottslingar involverade.
-  Typ av myndigheter (om möjligt).
-  Fordonets registrerings skylt eller andra kännetecken på myndigheterna.

Illegal invandringsinträde

Vad är hotet med illegalt invandrarinträde?

Hotet med illegalt invandrarinträde syftar på problemet med obehöriga personer som försöker ta sig in i länder genom att gömma sig i vägtransportfordon. Även om illegal migration förekommer globalt över olika transportsätt har den europeiska migrantkrisen särskilt påverkat landtransporten, särskilt väg- och järnvägstransport.

Kriminella nätverk som är inblandade i människosmuggling utgör ett betydande hot, där vissa nätverk enbart fokuserar på att underlätta illegala gränsövergångar genom vägtransportfordon. Detta innebär många utmaningar och risker för företag inom vägtransportbranschen. Några av konsekvenserna inkluderar skador på egendom och last, fysisk och psykisk våld mot förare och andra relaterade problem. Dessutom betraktas i fall där lasten är läkemedel eller livsmedelsprodukter eventuell intrång av illegala invandrare i lastutrymmet eller partiell öppning av förpackningar som förorening av lasten, och lasten aviseras från leverans.

För närvarande är debatterna om de problem som orsakas av illegala invandrare för europeiska vägtransportföretag inte särskilt väl adresserade.

Case example

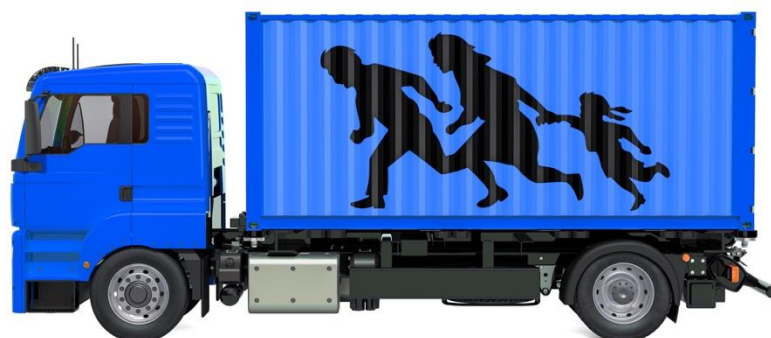
CRIMINAL NETWORK CHARGING UP TO EUR 20 000 PER MIGRANT

A criminal network facilitates the entry and secondary movements of irregular migrants in the EU. Migrants pay enormous sums to the smugglers to enter the EU clandestinely and move on to further destinations within its borders. The entire journey from the country of origin to the EU costs between EUR 15 000 and 20 000. The criminals advertise their illicit activities on various social media platforms to lure migrants, also by posting videos of successful transports. Migrants are moved along two main routes, either from Croatia via Slovenia to Italy, or from Serbia via Hungary to Austria.²⁵

Hur man förebygger hotet med illegalt invandrarinträde?

Fordonskontroller före och efter varje stopp

Det är vanligt att illegala invandrare försöker ta sig in i ett fordon när det är stoppat eller parkerat. För att förhindra detta rekommenderas det starkt att utföra fordonskontroller före och efter varje stopp. Denna praxis innebär att gå runt fordonet och se till att det inte finns några tecken på försök till inträde i lastutrymmet, kontrollera att förseglingarna är intakta och bekräfta att alla dörrar, lås och stängningar är ordentligt stängda och säkrade.



Hur man reagerar på hotet med illegalt invandrarinträde?

Gör

- Var närvarande när din lastbil lastas.
- Se till att förseglingar och lås/hänglås är låsta/fästa korrekt omedelbart efter lastning.
- När du tar över ansvaret för fordonet bör du säkerställa att fordonet inte innehåller obehöriga personer.
- Kontrollera ditt fordon och släpvagn för eventuella oregelbundenheter innan du fortsätter din resa. Förseglingar, lås, dörrar och presenningar är i gott skick och har inte manipulerats med.
- Kontrollera alltid perimetern runt ditt fordon efter en kort eller lång paus för att bekräfta att det inte finns några tecken på intrång och att förseglingar och lås är intakta.
- Kontrollera eventuella externa förvaringsutrymmen, axlar, verktyglådor, vindavvisare och fordonets undersida.

Undvik

- ANVÄND INTE oaviserade parkeringsplatser för korta och långa pauser på platser där risken för illegala invandrare att komma in i ditt fordon är hög.
- PLANERA INTE en paus/övernattning på avlägsna platser (t.ex. industriområden, rastplatser).
- GÖR INTE onödiga stopp under körning, särskilt om det inte finns planerade stopp eller nödsituationer.
- STOPPA INTE omedelbart om andra personer signalerar dig att göra det (t.ex. för ett "problem" med ditt fordon).
- ÖPPNA INTE släpvagnen/fordonet.
- NÄRMA DIG INTE personer som gömmer sig, håll avstånd.
- BERÖR INTE lasten/släpvagnen, eftersom det finns en risk för förorening.

Hur man rapporterar hotet med illegalt invandrarinträde?

Om du bevittnar eller misstänker hotet med illegalt invandrarinträde, kontakta omedelbart den lokala rättsmyndigheten eller akutnummer för nödtjänster i ditt område.

- 📍 Ge dem alla relevanta detaljer,
 - platsen
 - antalet inblandade personer
 - eventuell identifieringsinformation om de inblandade personerna
- 👤 Informera ditt avsändnings-/övervakningscenter eller de lämpliga personerna inom ditt företag om hotet med illegalt invandrarinträde.
- 📅 Följ ditt företags rutiner.

Brottslighet mot sista milens fordon

Vad är hotet med brottslighet mot sista milens fordon?

Hotet med brottslighet mot sista milens fordon syftar på kriminella aktiviteter som riktar sig mot fordon som vanligtvis används för sista milens leveranser i stadsområden. Dessa fordon, såsom minibussar eller mindre lastbilar med boxar, gör ofta flera stopp för att leverera eller hämta små paket. Sista milens fordon är särskilt sårbara för dessa typer av brott på grund av de frekventa stoppen och de värdefulla innehållen de transporterar.

Hur man förebygger hotet med brottslighet mot sista milens fordon?

- Anpassade säkerhetssystem på fordon (automatisk låsning, RFID-band, etc.)
Det finns många anpassade säkerhetssystem för att förebygga den här typen av incidenter, men den viktigaste åtgärden är alltid att låsa alla fordonets dörrar och aktivera de installerade säkerhetssystemen (intrångsfordonlarm, immobiliserare, etc.).

På senare tid har det införts några mycket avancerade säkerhetssystem (till exempel RFID-band på förarens handled som automatiskt låser fordonsdörrarna och aktiverar alla säkerhetssystem när föraren rör sig bort på ett visst avstånd från fordonet (t.ex. 3-5 m). Dessa band låser också upp fordonets lås när föraren når ett specifikt avstånd från det.

Hur man svarar på hotet med brottslighet mot sista milens fordon?

Gör





- Alltid lås din bil och aktivera alla säkerhetssystem när du stannar för att göra en leverans.
- Var vaksam och medveten om din omgivning.
- Identifiera misstänkt beteende eller individer och rapportera alla ovanliga händelser till ditt övervaknings-/avsändningscenter.
- Ha med dig en fjärrkontroll för att aktivera sirenen i fordonets larm om du ser på avstånd att någon antingen har gått in i ditt fordon eller försöker ta sig in i det.

Undvik

- PARKERA INTE långt bort från leveransplatsen och behöva gå långt med paketen i händerna för att nå leveransplatsen.
- ÖVERBELASTA INTE dig själv med paket när du kliver ur ditt fordon för leverans, så att dina händer är upptagna och du försöker stänga fordonets dörrar med ditt ben.
- LÄMNA INTE dina nycklar i tändningslåset eller obemannade inuti fordonet, inte ens under en kort tid.
- LÄMNA INTE några värdefulla föremål, inklusive personliga tillhörigheter eller högvärdiga paket, synliga från utsidan av fordonet.
- DEL INTE specifik leveransinformation, såsom exakta innehåll, adresser eller leveransschema, med personer som inte är auktoriserade eller involverade i leveransprocessen.

Hur man rapporterar hotet med brottslighet mot sista milens fordon?

Att rapportera hotet med brottslighet mot sista milens fordon är avgörande för att hantera situationen och säkerställa din egen säkerhet, ditt fordon och de paket som levereras. Så här kan du rapportera sådana incidenter:

-  Meddela omedelbart den lokala rättsmyndigheten eller nödtjänsterna i ditt område.
-  Ge dem alla relevanta detaljer, inklusive platsen, beskrivning av händelsen och all identifieringsinformation om de inblandade individerna.
-  Rapportera hotet med brottslighet mot sista milens fordon till ditt avsändnings-/övervakningscenter eller de lämpliga personerna inom ditt företag.
-  Försök att bevara alla bevis relaterade till händelsen, såsom fotografier, videor eller annat fysiskt material som kan vara användbart för utredningen.

Cyberbrott och läcka av informationssäkerhet

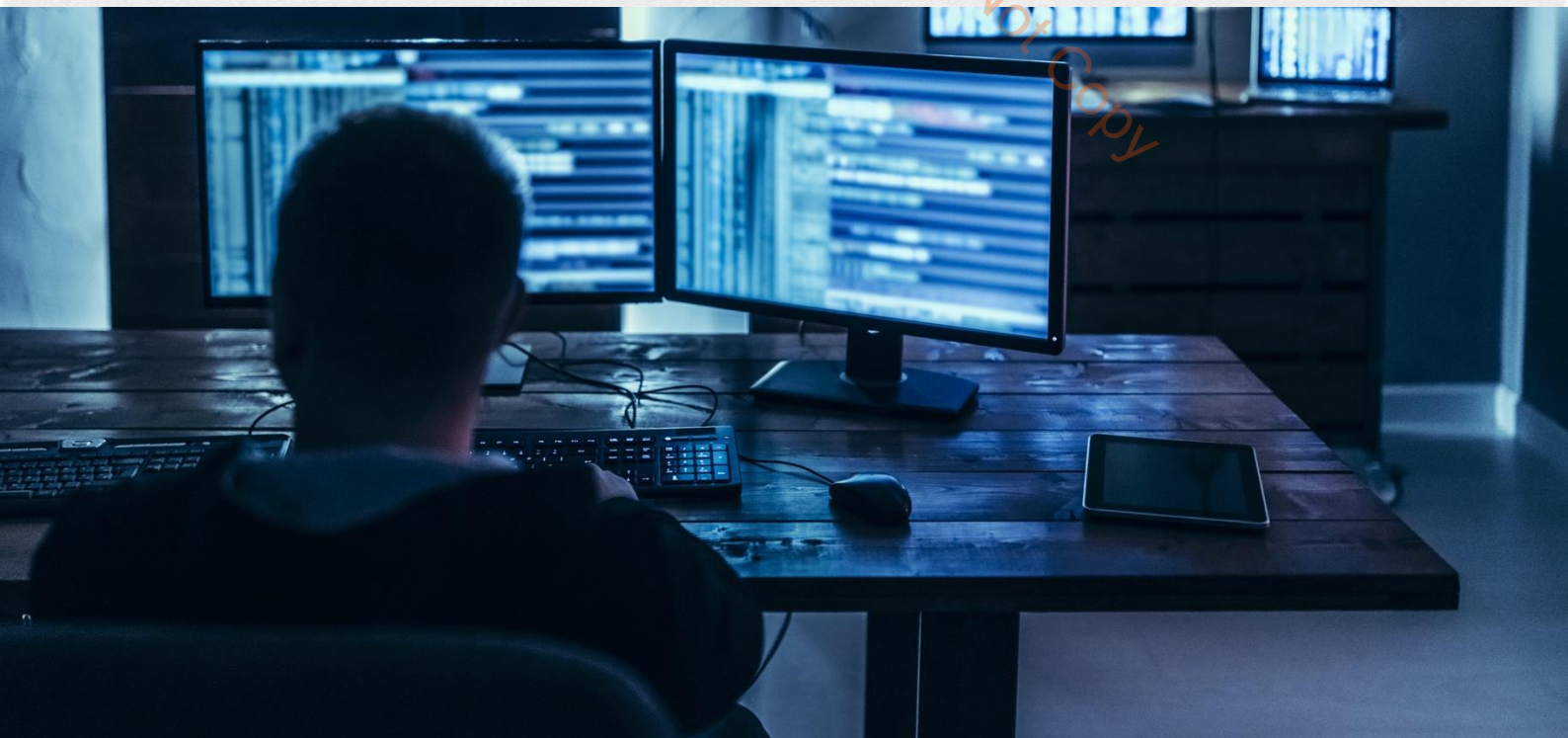
Vad är hotet med cyberbrott och läcka av informationssäkerhet?

Inom försörjningskedjans säkerhet när vi talar om cyberbrott, menar vi antingen attacker mot informationssystem som syftar till att stjäla känslig lastinformation (t.ex. ruttens ursprung och destination, typer och värden av last) eller oavsiktlig läcka av information från logistikleverantörer eller förarna. I det här dokumentet kommer vi att fokusera på oavsiktlig läcka av information från förare via deras sociala mediekonton eller e-postkonton.

Hur man förebygger hotet med cyberbrott och läcka av informationssäkerhet?

Det kräver starka försvarsmekanismer, med förståelse för att mänsklig övervakning fortfarande utgör den svagaste länken. Brottslingar utnyttjar ofta sårbarheter genom phishing-e-postmeddelanden, skadliga dokumentfiler, social ingenjörskonst och opatchad programvara och hårdvara.

- Var vaksam för phishing-attacker på telefoner och surfplattor
Du bör alltid validera inkommande e-postmeddelanden, särskilt de som ber dig använda en länk för att gå vidare. På så sätt kan brottslingar få åtkomst till information som lagras på din telefon, inklusive rut- och lastinformation.
- Skydd av leveransinformation och dokument
Brottslingar kan effektivt organisera en attack genom att få åtkomst till leveransdokument, som innehåller vital information. Till exempel innehåller ett CMR-dokument detaljer som lastens ursprung, destination, typ, kvantitet, förarens namn, sigillnummer och mer. Om brottslingar riktar in sig på din last, är åtkomst till denna information tillräckligt för dem att börja organisera attacken.
- Behov av att veta grunderna
Leveransdokument är inte det enda sättet för brottslingar att få tillgång till ovanstående information. Många gånger är den okontrollerade distributionen av denna information (antingen muntligt eller skriftligt) bland anställda, särskilt de som inte bör känna till denna information, tillräcklig för välutbildade personer att extrahera denna information och tillhandahålla den till brottslingarnas grupper.



Hur man reagerar på hotet med cyberbrott och läcka av informationssäkerhet?

Om du misstänker läckage av information antingen från datorsystem eller från okontrollerad dokumentation, måste du rapportera detta till ditt avsändningscenter och be dem om instruktioner om hur man mildrar dess konsekvenser.

Hur man svarar på hotet med cyberbrott och läcka av informationssäkerhet?

Gör



- Kontrollera alltid avsändaruppgifterna innan du klickar på en länk i ett mottaget e-postmeddelande.
- Skydda leveransdokumenten medan de är under din vårdnad.
- Rapportera eventuellt ovanligt beteende hos din mobiltelefon och be din IT-avdelning att kontrollera den.
- Rapportera eventuella misstänkta aktiviteter eller händelser till din organisations IT-avdelning eller säkerhetsteam.
- Använd starka, unika lösenord för alla dina konton och åtkomst till mobiltelefonen.

Undvik

- BESVARA INTE något inkommande samtal från okända (vanligtvis från utlandet) nummer.
- DEL INTE någon information om dina rutter, inklusive lasttyp, uppskattat värde, ursprung, destination och pauser, med personer som inte behöver denna information.
- PUBLICERA INTE jobbrelaterad information och bilder på sociala medier.
- LÄMNA INTE dina enheter obemannade eller olåsta, särskilt på offentliga platser.
- ANTA INTE att du inte är ett mål - cyberbrottslingar kan rikta in sig på vem som helst.

Hur rapporterar man cyberbrott och hot om informationssäkerhetsläckor?

Om du misstänker att du har blivit offer för ett cyberbrott relaterat till din transportväg eller om du har upptäckt en läcka av detaljer om din resplan, rapportera det omedelbart till din dispatcher/övervakare. Inkludera följande detaljer i din rapport:

-  Hur du identifierade läckan eller misstänkt cyberbrott.
-  Vilken specifik information som läcktes eller komprometterades.

Dispatch- eller övervaknings- och responscenters funktioner och stöd till förare

Övervaknings- och responscenters spelar en avgörande roll för att säkerställa säkerheten och tryggheten för tillgångar, såsom lastbilar eller släpvagnar, under transport. Det är viktigt att förstå skillnaden mellan spårning och övervakning:

- Spårning: Spårning innebär att veta status eller plats för din lastbil och/eller släpvagn. Det ger realtidsinformation om fordonets position, vilket möjliggör synlighet och spårning av dess rörelser.
- Övervakning: Övervakning går utöver spårning genom att jämföra den faktiska statusen för din lastbil och/eller släpvagn, såsom dess plats, med den planerade eller förväntade statusen. Det innebär att ha en fördefinierad plan eller rutt och kontinuerligt jämföra de faktiska data som tillhandahålls av spårningssystemet med de förväntade data.

Det är viktigt att notera att övervakning endast kan ske när det finns en fördefinierad plan eller rutt på plats. Utan korrekt planering finns det inget att övervaka. Därför förlitar sig övervakningscentren på noggrann planering och realtids spårningsinformation för att effektivt övervaka tillgångarnas framsteg och säkerhet under transporten.

Observera att även vid transporter där det inte finns en dedikerad övervakningsfunktion för att övervaka ruttens utförande, finns det alltid en typ av övervakning från transportörens dispatchers mot förarna och lasten för att säkerställa att inga oväntade händelser inträffar under transporten. Därför, tänk alltid på att det finns någon på hemmakontoret eller övervakningscentret som ser efter din säkerhet och lastsäkerhet.

Rutten är en kombination av:

- en lastbil (med släpvagn, om tillämpligt),
- en förare,
- en startpunkt,
- en destination,
- en avgångstid,
- en beräknad ankomsttid, och
- Planerade stopp vid fördefinierade platser med tillhörande tidsintervall för varje stopp däremellan.



Det finns flera tekniker/lägen för övervakning:

- **Aktiv övervakning:** Övervakningsstationen spårar och övervakar aktivt tillgångens plats och framsteg under hela ruttens varaktighet i realtid.
- **Passiv övervakning:** Övervakningsstationen kontrollerar och registrerar utförandet av rutten en eller ett fåtal gånger under dess varaktighet.
- **Övervakning genom undantag:** Övervakningsstationen får endast larm eller meddelanden när det sker avvikelser från den planerade rutten eller schemat.
- **Övervakning per tidsintervall:** Övervakningsstationen kontrollerar utförandet av rutten vid regelbundna tidsintervall, såsom varje 15, 30 eller 60 minuter. Den verifierar om tillgången följer den planerade rutten och håller sig till det förväntade schemat inom dessa fördefinierade intervall.
- **Övervakning per ruttmilstolpe:** Övervakningsstationen kontrollerar varje specifik milstolpe (t.ex. ankomst till en specifik plats) för att säkerställa att rutten genomförs enligt plan.

I princip är ansvaret för en övervakningsstation att:

- Ta emot,
- Verifiera och
- Svara på en larmhändelse (avvikelse från den planerade rutten) inom en överenskommen tidsperiod.

Verifiering utförs vanligtvis genom telefonkommunikation mellan övervakningsstationen och föraren, med hjälp av ett specifikt nyckelord. Föraren måste inkludera nyckelordet i sitt svar för att identifiera sig själv och bekräfta sin status. Dock kan föraren på högriskrutter få instruktioner att utesluta nyckelordet vid verkliga larm, såsom när hen befinner sig i en gisslansituation.

När föraren kan kommunicera med övervakningsstationen är det avgörande att hen tillhandahåller korrekt information. Detta säkerställer att operatören på övervakningsstationen fullt ut kan förstå situationen och initiera lämplig svarspolicy.

I händelse av att föraren befinner sig i en gisslansituation måste fördefinierade svarspolicys vara på plats. Dessa protokoll beaktar att föraren kanske inte kan ge en korrekt beskrivning av situationen på grund av de fientliga omständigheterna. Övervakningsstationen kommer att initiera de nödvändiga åtgärderna baserat på de etablerade protokollen för att säkerställa förarens och lastens säkerhet.

Europeiska nödnummer

Country	Police	Emergency/Ambulance Services
Austria	133 or +43 59 133	112
Belgium	101	112
Bulgaria	112 or 166 or 02 98 28 363	112 or 160
Croatia	112 or 192	112 or 194
Cyprus	112 or 199	112 or 199
Czech Republic	112 or 158	112 or 155
Denmark	112 or 114	112
Estonia	112	112
Finland	112	112
France	17 or 112	15 or 112
Germany	110	112
Greece	100 or 112	166 or 112
Hungary	107 or 112	104 or 112
Ireland	112 or 999	112 or 999
Italy	112 or 113	112 or 118
Latvia	110 or 112	113 or 112
Lithuania	112	112
Luxembourg	113	112
Malta	112	112
Netherlands	112	112
Poland	112 or 997	112 or 999
Portugal	112	112
Romania	112	112
Spain	112 or 091 or 092	112 or 061
Slovakia	112	112 or 155
Slovenia	112 or 113	112
Sweden	112	112
Switzerland	117	144
UK	999	999 or 111



Viktiga regler för förare

Här är några viktiga regler för förare för att skydda dig och din last från organiserad eller opportunistisk brottslighet. Följ instruktionerna nedan utan undantag:

1. Använd motorvägar och huvudvägar för långa resor till stora destinationer. Undvik om möjligt sekundära vägar och genvägar.
2. Förare och medhjälpare ska inte diskutera eller lämna ut någon information om sin försändelse till andra parter eller personer medan de är på väg till sina destinationer. Det är även bäst att undvika att lämna jobbrelaterad information (rutter, last etc.) i personliga sociala mediekonton.
3. Bär aldrig obehöriga passagerare. Plocka aldrig upp liftare.
4. Se alltid till att ditt fordon är säkert, även när du kör.
5. Lämna aldrig fordonet eller försändelsen obebakad vid något tillfälle. Avbrott för vila (som måltider och/eller toalettbesök) ska inte äventyra denna process – om två förare är ombord måste en av dem alltid vara kvar med fordonet. Om fordonet måste stanna under en längre tid, kontakta dispatch eller övervakningscenter för att säkerställa att du endast parkerar på godkända säkra platser, såsom certifierade parkeringsområden, betalstationer eller vid polisstationer i mindre städer eller byar. Res i konvojer när det är möjligt.
6. Om det är oundvikligt att parkera utanför ett säkert/skyddat område, vidta ytterligare säkerhetsåtgärder som att parkera med bakhjulen mot en annan lastbil eller en vägg.
7. Om leverans inte kan genomföras måste råd sökas från hemmabasen eller övervakningscentret om vad man ska göra med lasten.
8. Insistera alltid på tydliga, precisa mottagningsbevis. Föraren bör kontrollera ID för personen som tar emot godset på kundens vägnar innan några paket överlämnas. Utmana eventuella sista minuten-ändringar.
9. Var försiktig med oombedda erbjudanden om hjälp från okända personer.
10. Var försiktig med signaler från andra förare om att något är fel med ditt fordon.
11. Brottslingar försöker ibland utge sig för att vara poliser eller andra myndighetspersoner; därför bör extra uppmärksamhet ägnas åt situationer där man oväntat utmanas av myndigheter. Förare bör meddela sin dispatch eller övervakningscenter om sin plats innan de stannar sitt fordon om det är säkert att göra det.
12. Håll regelbunden kontakt med dispatch/basen. Föraren bör ha flera metoder att kontakta dispatch/bas (t.ex. teleprinter, mobiltelefon, RF-radio osv.). Föraren ska ha med sig mobiltelefon eller annan kommunikationsenhet vid alla tillfällen.
13. Håll koll på dina backspeglar och notera eventuella fordon som kan följa din lastbil. Rapportera eventuella misstänkta fordon eller händelser omedelbart.
14. Ha med dig ett säkerhetsinformationskort för förare inklusive alla nödnummer.
15. Var uppmärksam när du tar emot inkommande samtal eller e-post från okända nummer/konton.

Bryt aldrig mot reglerna. Dessa regler utgör grunden för att ta över lasten och utföra transporten!

References

1. European Parliament study on Organized Theft of Commercial Vehicles and their Loads in the European Union
2. International Journal of Retail & Distribution Management Vol. 43 No. 3, 2015 pp. 204-220, Cargo Theft at non-secure parking locations, ©Emerald Group Publishing Limited, 0959-0552, DOI 10.1108/IJRDM-06-2013-0131
3. TAPA EMEA, 18 MONTHS OF CARGO CRIME EUROPE, MIDDLE EAST & AFRICA REGION, REPORTING PERIOD TO 30 JUNE 2022
4. The International Journal ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES ISSN 2345-0282, 2018 Volume 5 Number 3 (March) PECULIARITIES OF ILLEGAL IMMIGRANT'S INTRUSIONS INTO ROAD FREIGHT TRANSPORT UNITS IN THE FRANCE - UK CORRIDOR
5. Europol DECODING THE EU'S MOST THREATENING CRIMINAL NETWORKS, PDF | ISBN 978-92-95236-25-7 | DOI: 10.2813/811566 | QL-05-24-250-EN-N
6. Cyber-Security and Information Warfare, Copyright © 2019 by Nova Science Publishers, Inc. pp. 201, A Case Study Analysis of Attacks and Losses in the Supply Chain with the Use of GPS or GSM Jammers by the Attackers Panayiotis Laimos, Michalis Chronopoulos, Chrysanthi Laimou and Nikoleta Atanasova, ISBN: 978-1-53614-386-7
7. <https://www.fleeteurope.com/en/technology-and-innovation/global/features/ransomware-rise-again-causing-shattering-damages-fleets?t%5B0%5D=Fleet%20Management&curl=1>
8. Europol Internet Organised Crime Threat Assessment (IOCTA) 2023, Luxembourg: Publications Office of the European Union, 2023, PDF ISBN: 978-92-95220-83-6 ISSN: 2363-1627 doi:10.2813/587536 QL-AL-23-001-EN-N, © European Union Agency for Law Enforcement Cooperation, 2023
9. <https://www.cybertalk.org/2021/07/28/ransomware-attacks-on-the-transportation-industry-2021/> Ransomware attacks on the transportation industry, 2021
10. <https://www.telegraph.co.uk/news/uknews/immigration/11694134/Calais-crisis-Illegal-immigrants-shut-down-all-Channel-traffic.html>
11. BSI and TT Club 2023 Cargo Theft Report, April 2024

Ansvarsfriskrivning för Förarhandboken om Säkerhet

Detta dokument om förarvägledning inom säkerhet tillhandahåller användbara tips och information som har sammanställts enligt bästa kännedom och övertygelse, baserat på erfarenhet och bakgrundsinformation. Ämnena har valts utifrån aktuella trender och behov år 2024, klaggjorda och publicerade av TAPA EMEA. Föreningen fungerar som en supporter av branschen och den anslutna leveranskedjan i detta sammanhang, med syftet att minimera risken för förluster från de risker som nämns här.

Observera att antalet och listan över de punkter som nämns kanske inte är heltäckande, och inte alla potentiella faror eller ytterligare farliga risker listas här.

Rekommendationerna om åtgärder för att undvika eller korrekt beteende som nämns i dokumentet återspeglar också expertisen hos TAPA EMEAs experter som varit involverade i skapandet av detta förarhandboksdocument om säkerhet.

Detta dokument tjänar enbart som stöd och en åtgärd för att skapa medvetenhet för förare av allmän last och HVC. Ansvar för genomförande, korrekt användning och rätt tillämpning åligger läsaren, användaren eller branschen, inklusive logistikleverantörerna.

Användaren/läsaren av dokumentet/policyn är medveten om de åtgärder som följer. Varken TAPA EMEA eller de medverkande experterna ådrar sig något ansvar, skyldighet eller ansvar i skadestånd som rör ämnena som nämns här, deras hantering eller de data som tillhandahålls, vilket är baserat på förtroende för referenser som nämns och tillhandahålls av tredje part.

Publicerings- och upphovsrättsinformation

Upphovsrättsnotisen från TAPA EMEA som visas i detta dokument anger när dokumentet senast utfärdades.

@ TAPA EMEA 2024

Ingen upphovsrätt utan TAPA EMEA tillstånd utom enligt tillåtet enligt upphovsrättslagen.

Publiceringshistorik

Första gången publicerad i juni 2024.

Nuvarande utgåva publicerades i juni 2024.

