Cyber Safe voor de Transport & Logistiek

Bescherm de marges tegen de financiële gevolgen van cybercriminaliteit

TMS, WMS, FMS... De transport- en logistieksector is in hoog tempo gedigitaliseerd en dus sterk afhankelijk geworden van technologie. Waar vroeger files of materiaalpech vertraging veroorzaakten, kan een cyberaanval leiden tot stilstaande vrachtwagens en opstoppingen in magazijnen. Bedrijfsstilstand, kosten voor expertise, herstelkosten en geschillen achteraf komen direct ten laste van de nettowinst.

Baobab Cyber Safe biedt voor de transport- en logistieksector een cyberverzekering met unieke clausules voor de transportsector, zodat de financiële en operationele gevolgen van een storing op kantoor, in het warehouse en onderweg effectief worden afgewend.



Kenmerken van de transport- en logistieksector

Strakke Planningen & Just-in-Time Ketenintegratie

Transporteurs en logistiek dienstverleners werken met strakke venstertijden en directe ketenkoppelingen (EDI/API). Een ransomware-aanval of cloud-storing in het TMS of plansysteem leidt direct tot een kettingreactie van vertragingen en opstoppingen bij distributiecentra en klanten.

Ketenafhankelijkheid & Contractuele aanspraken

Opdrachtgevers stellen strenge leveringsvoorwaarden en hanteren harde boetebepalingen bij vertraagde levering. Als zendingen niet tijdig worden geregistreerd of afgeleverd doordat systemen plat liggen, lopen logistieke bedrijven tegen omvangrijke claims en contractbreuk aan.

OT & Magazijnautomatisering

Distributiecentra draaien steeds meer op geautomatiseerde processen. Een cyberaanval op deze OT-infrastructuur kan systemen ontregelen of fysieke beschadigingen tot gevolg hebben, waardoor het complete warehouse stilvalt.

Praktijkvoorbeeld / Scenario

Ransomware gijzelt TMS, sorteercentrum stokt en ritten vallen uit

Na een phishingmail raakt het centrale netwerk van een logistiek dienstverlener besmet met ransomware. Het TMS en WMS zijn onbereikbaar en digitale vrachtbrieven kunnen niet meer worden gegenereerd. Vrachtwagens kunnen niet rijden en de automatische sorteerinstallatie in de centrale overslaghal schakelt zichzelf uit. Opdrachtgevers zijn gedupeerd door de gemiste leveringen aan distributiecentra, terwijl bederfelijke goederen in het magazijn verminderd verkoopbaar raken.

Dekkingsoverzicht & Acceptatievoorwaarden

Wat is standaard gedekt bij Baobab?

- ✓ **24/7 Noodhulp & Response Team:** Directe bijstand door forensische IT-experts en juristen. De kosten in de eerste 48 uur zijn volledig vrijgesteld van het eigen risico. Kosten voor crisisinterventie en onderhandeling met criminele groepen worden vergoed.
- ✓ **Herstel & Data-reconstructie:** Volledig herstel van data, software, applicaties, TMS/WMS-configuraties en aangestuurde OT-systemen op kantoor en operationele vestigingen.
- ✓ **Bedrijfsschade & Vaste Kosten:** Dekking voor brutowinstderving (vaste doorlopende kosten zoals personeelskosten en huurverplichtingen plus gederfde nettowinst). Gedekt bij cyberincidenten, menselijke fouten en technische storingen (ook cloud-uitval) al na een wachttijd van 8 tot 12 uur.
- ✓ **Aansprakelijkheid:** Naar aanleiding van een datalek of bijvoorbeeld transmissie van een virus.

Verzekeringsdekking met bijzondere relevantie voor Transport & Logistiek

- ✓ **Pech! Lading weg? Verlies van cargo als gevolg van een cyberincident, bijvoorbeeld een gemanipuleerde vrachtbrief (tot €250.000):** Vergoeding bestaat tot de geldende bedragen in CMR/AVC, dus tot maximaal €10,00 per kilogram brutogewicht van de weggenomen lading.
- ✓ **Zaakschade aan goederen in het logistiek proces (tot € 250.000):** Dekking voor zaakschade aan eigen goederen of handelsvoorraad, waaronder beschadiging, contaminatie, bederf of andere vormen van waardevermindering ontstaan tijdens opslag of overslag door een cyberincident.
- ✓ **OT-bricking (tot € 250.000):** Vergoeding voor reparatie, herprogrammering en vervanging van Operationele Technologie (zoals PLC's, SCADA-componenten en sensoren van sorteer- en conveyorsystemen).
- ✓ **Aangepast op de Cyberbeveiligingswet (NIS-2):** Verweerkosten en eventuele bestuurlijke boetes voor bedrijven die onder de nieuwe Cyberbeveiligingswet vallen.
- ✓ **Contractuele boetes (tot € 500.000):** Dekking voor contractuele boetes wegens late levering of niet-nakoming van contractvoorwaarden als direct gevolg van een cyberincident.

Acceptatievoorwaarden & Risicoprofiel

Baobab hanteert een transparante premieopbouw gebaseerd op het beveiligingsniveau, omzet en de specifieke sectorclassificatie. De sector transport & logistiek heeft een lage premieopslag in het Baobab broker portaal en Baobab kent dan ook lage basispremies toe. Let op! Wij kunnen geen luchttransport verzekeren.



Minimumeisen voor acceptatie van de verzekering

- **Baobab Deepscan:** Positief resultaat van de externe veiligheidsscan.
- **Back-ups:** Minimaal wekelijks en opgeslagen op een afgescheiden plek.
- **Multi-Factor Authenticatie (MFA):** op externe toegang, op vertrouwde apparaten volstaat een complex wachtwoord.
- Voor bedrijven met omzetten boven de €100 miljoen bestaan 2-5 aanvullende vereisten.



Jackie van Ginkel
Senior Broker Manager
jackeline.vanginkel@baobab.io
+31 6 21 45 66 08

Tim van Lier
General Manager
tim.vanlier@baobab.com
+31 6 26 73 95 95

