

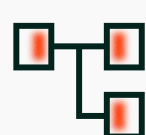
Cyber Safe voor de Koelvries-sector: Voorkom Bederf, Verzeker Continuïteit

De koel en vrieslogistiek sector is een geliefd doelwit geworden voor cybercriminelen. In de wereld van koel- en vrieslogistiek is tijd de grootste vijand. Waar een IT-storing bij een gemiddeld kantoor al behoorlijk vervelend is, kan een aanval bij een koel-vrieshuis binnen enkele uren leiden tot schade aan voorraden, contractbreuk en logistieke problemen.

Baobab Cyber Safe heeft voor de koelvries-sector een **branche-specifieke verzekeringsdekking** ontwikkeld zodat de financiële gevolgen van een cyberaanval kunnen worden afgewend.



Kenmerken van de koelvries-branch:



Bederfelijkheid

Hackers richten zich op koel-vriesbedrijven vanwege de afhankelijkheid van koelingsbeheersystemen (ICS/SCADA) en vergankelijkheid van de goederen die zich in het logistieke proces bevinden. Afpersing werkt nu eenmaal beter onder **tijdsdruk**.



Just-in-Time

Marge voor vertraging is nihil. Een hack van het Warehouse Management System (WMS) heeft **direct gevolgen** voor de keten en levert problemen op met contractanten.



Verouderde techniek

Koelinstallaties hebben een levensduur van tientallen jaren en zijn ontworpen om betrouwbaar te koelen – niet om zich te verdedigen tegen hackers. **Segmentatie** is van cruciaal belang zodat een simpele phishing-mail bij de receptie niet leidt tot een uitschakeling van de vriescellen.

Baobab Cyber Safe in actie: Onderbroken cold chain monitoring en voorraad-blindheid

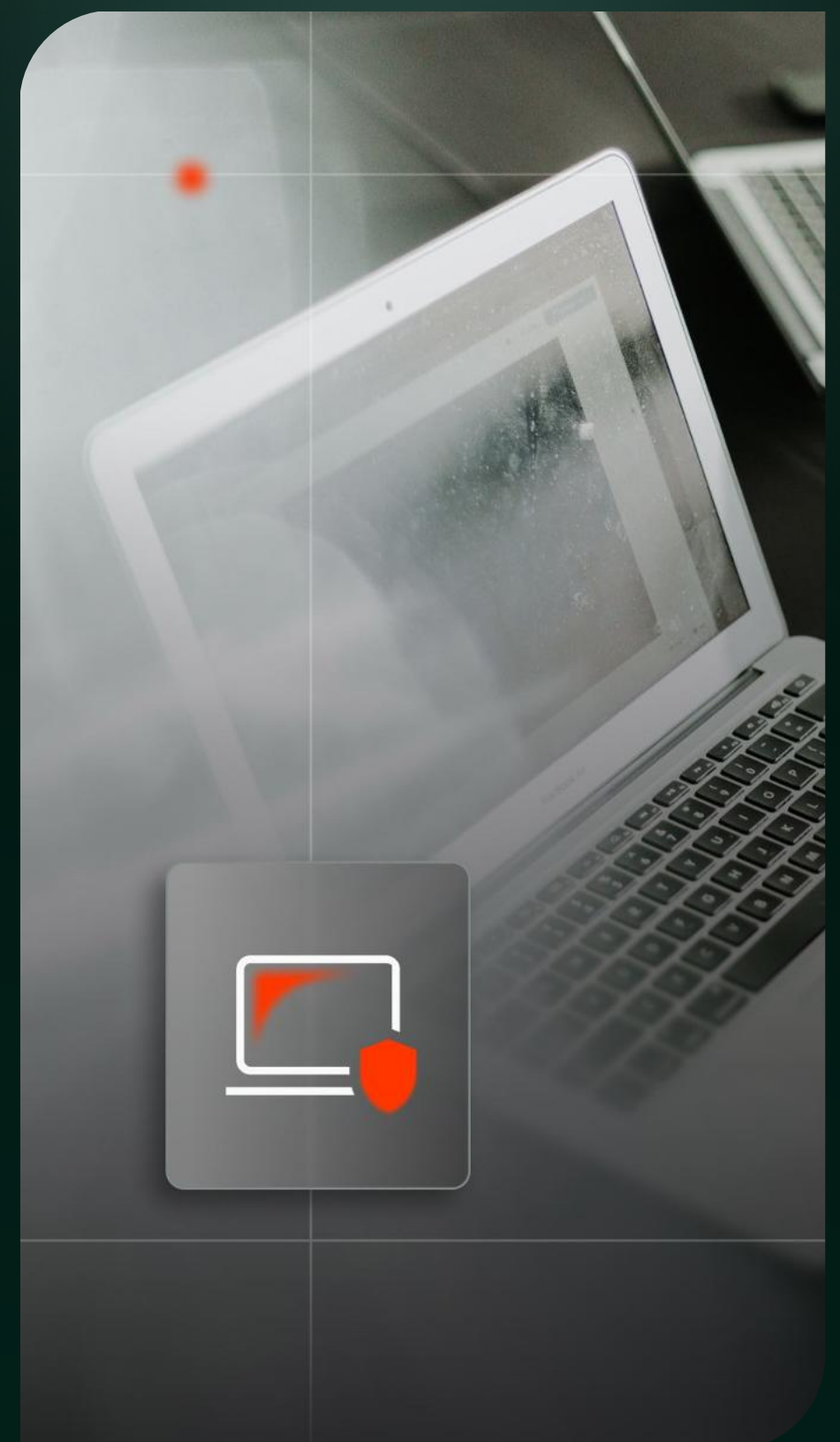
Na een geslaagde ransomware-aanval, is toegang tot het Warehouse Management Systeem (WMS) niet beschikbaar. Zonder toegang tot deze data **ontstaat voorraadblindheid**: er is geen Track & Trace mogelijk, goederen kunnen niet worden uitgeleverd waardoor vrachtwagens komen stil te staan bij de poort van het koelvrieshuis.

Wat is standaard gedekt bij Baobab?

- ✓ **Noodhulpkosten** – alle kosten voor forensische experts, advocaten enz., vrijgesteld van het eigen risico tijdens de eerste dagen na ontdekking. Isolatie, mitigatie en onderzoek.
- ✓ **Onderhandeling** met ransomware-criminelen en eventuele afpersingsbetaling in cryptovaluta.
- ✓ **Herstel van gegevens en systemen**, apps en software (ook cloud-software en OT-systemen)
- ✓ **Bedrijfsschade** volgens brutowinst-formule waardoor naast de netto-winst ook doorlopende kosten meeverzekerd zijn.

Verzekeringsdekking met bijzondere relevantie voor koelvries-sector:

- **Zaakschade** – door bederf of contaminatie (tot EUR 250.000 meeverzekerd), aan goederen in productie en voorraad, bijvoorbeeld afgekeurde goederen door een onderbreking in de cold chain-monitoring.
- **Bedrijfsschade** die ontstaat door cyberincidenten, menselijke fouten, technische problemen en fysieke gebeurtenissen: oververhitting, over/onderspanning, elektrostatische ontlading of statische elektriciteit, komt voor vergoeding in aanmerking.
- **Contractuele boetes** (tot EUR 500.000), die verbeuren in verband met late levering van goederen en/of diensten door een cyberincident of bedienings- en programmeerfout.
- De koelvries-sector is onderworpen aan de **Cyberbeveiligingswet** (NIS-2), **verweerskosten** en eventuele **boetes** opgelegd door de toezichthouder zijn in beginsel gedekt.
- Operationele Technologie (ICS/SCADA) wordt gezien als onderdeel van het verzekerde computernetwerk, waardoor **een cyberincident gericht tegen de OT-omgeving ook gedekt is**.



Wat zijn de voorwaarden voor acceptatie?

- **Positief resultaat “Deepscan”**, waarbij Baobab de verkenning van een hacker nabootst door het extern waarneembare aanvalsoppervlak te scannen. Let op! Als onderdeel van de preventieve service blijft Baobab uw domein scannen tijdens de looptijd van de verzekering. Zo bent u altijd op de hoogte van actuele dreigingen
- **Wekelijkse back-ups**
- **Multi-Factor Authenticatie (MFA)** wanneer ingelogd kan worden op afstand
- Vanaf EUR 100 miljoen: **Endpoint Detection Response/ Managed Detection & Reponse** OF gebruik van **antivirus** software
- **Netwerksegmentatie** tussen IT en OT (Operationele Technologie), dus bijvoorbeeld de koelingsbeheersystemen of gebouwbeheersystemen

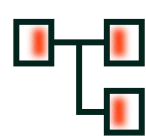


Is fraude ook gedekt?

Social Engineering komt steeds vaker voor. Als een hacker toegang heeft tot uw netwerk (bijvoorbeeld door een gehackt e-mailadres) en u daardoor beweegt tot het doen van een betaling aan een fraudeur, **is deze schade tot EUR 250.000** meeverzekerd als onderdeel van de polis.

Let op! Polishouders bij Baobab worden gemonitord op darkweb-activiteit, **u wordt op de hoogte gesteld als inloggegevens worden aangeboden op het darkweb.**

Voordelen bij Baobab Risk Solutions:



Professionele support

In-house **specialisten** die u te woord staan bij actieve security-problemen.



Uitgebreide dekking

Ruime dekking **voor digitale gevaren.**



Risico's in zicht

Continue monitoring van het externe aanvalsoppervlak.

Contactpersonen



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



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