

Cyber Safe voor de Maritieme Sector

Blijf op koers en verzeker continuïteit op het water

De maritieme sector digitaliseert in hoog tempo. Navigatiesystemen, geautomatiseerde besturing en andere gekoppelde Operational Technology (OT) maken schepen efficiënter, maar ook kwetsbaarder voor cyberincidenten. Een cyberaanval op een rederij of schip kan binnen enkele uren leiden tot stilliggende schepen en dus liggeld, gemiste havenvensters, boetes en zelfs aanvaringen.

Baobab CyberSafe biedt een branche-specifieke dekking voor de maritieme sector die de financiële en operationele impact van een aanval minimaliseert. Met dekkingen die in de reguliere verzekeringsmarkt niet beschikbaar zijn.



Kenmerken van de maritieme sector:



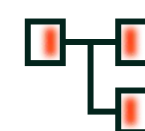
Stilliggende schepen en fysieke schade

Een gehackt computersysteem aan boord kan verstrekende gevolgen hebben. Schepen zijn in toenemende mate afhankelijk van digitale systemen en een cyberincident kan tot gevolg hebben dat het schip stil komt te liggen. In ernstige gevallen kan een cyberincident zelfs fysieke schade veroorzaken.



Schade in de Bermudadriehoek: casco, aansprakelijkheid en cyber

Traditionele cyberverzekeringen sluiten materiële schade uit. Tegelijkertijd dekken reguliere casco- en aansprakelijkheidsverzekeringen cyber-gerelateerde schade in de regel niet. Hierdoor ontstaat een stuk onverzekerbare schade voor reders en maritieme ondernemingen. Baobab CyberSafe komt de maritieme sector tegemoet.



Integratie van IT en Operationele Technologie (OT)

De grens tussen kantoor-IT en Operationele Technologie op schepen (navigatie, voortstuwing, ladingbeheersing) vervaagt. Een digitale kwetsbaarheid aan wal kan zo direct de controle over het schip op het water in gevaar brengen.

Praktijkvoorbeeld / Risicoscenario

Ransomware op de wal-infrastructuur

Na een geslaagde ransomware-aanval op de wal-infrastructuur van een rederij is er geen verbinding meer mogelijk met de vloot-managementsystemen. Zonder deze data is er geen inzicht in posities. Schepen kunnen havens niet veilig binnenlopen, de logistieke keten stopt en havenvensters worden gemist. De operatie kan pas na dagen worden hervat.

Dekkingsoverzicht & Acceptatievoorwaarden

Wat is standaard gedekt bij Baobab?

- ✓ **Noodhulpkosten:** Directe toegang tot maritieme cyber-experts en advocaten, vrijgesteld van het eigen risico tijdens de eerste 72 uur. Isolatie van de aanval op zowel wal- als schipssystemen.
- ✓ **Onderhandeling & Losgeld:** Professionele begeleiding bij ransomware-incidenten en dekking voor eventuele afpersingsbetalingen in cryptovaluta om de operatie weer vlot te trekken.
- ✓ **Herstel van Systemen (inclusief verbetering):** Herstel van data, scheepssoftware en navigatiesystemen, inclusief verbeteringskosten om herhaling te voorkomen.
- ✓ **Bedrijfsschade (Gross Profit):** Vergoeding van nettowinst en doorlopende vaste kosten (zoals bemanning en lease) wanneer de vloot of de wal-organisatie door een cyberincident stil komt te liggen.
- ✓ **Extra kosten:** alle redelijke en noodzakelijke kosten die worden gemaakt om operationeel te blijven en schade te beperken (inkoop extra tijdsloten, extra arbeidsuren, liggeld).

Verzekeringsdekking met bijzondere relevantie voor maritieme-sector:

- ✓ Casco-schade (hull) (tot EUR 250.000) – voor fysieke schade aan het schip of schade als aansprakelijkheid als gevolg van een aanvaring door een cyberincident. Deze dekking is uniek en uitgesloten op andere verzekeringen. Deze dekking is vanaf €300 per schip verkrijgbaar.
- ✓ Contractuele boetes (tot EUR 500.000), die verbeuren in verband met late levering van goederen door een cyberincident of bedienings- en programmeerfout.
- ✓ Zaakschade – door bederf of contaminatie (tot EUR 250.000), aan goederen in het logistieke proces.
- ✓ NIS-2 – de maritieme sector is (gedeeltelijk) onderworpen aan de Cyberbeveiligingswet (NIS-2), verweerskosten en eventuele boetes opgelegd door de toezichthouder zijn behoudens uitzonderingen gedekt.
- ✓ Navigatietechnologie 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 verkenningfase 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. (Indien geen website beschikbaar is, worden de minimumcriteria extra van belang voor acceptatie).
- Wekelijkse back-ups.
- Multi-Factor Authenticatie (MFA) wanneer ingelogd kan worden op afstand.
- Vanaf €100 miljoen omzet worden aanvullende eisen gesteld, maar de aanvraagprocedure is 80% korter dan gemiddeld.
- Netwerksegmentatie tussen kantoor-IT en Operationele Technologie (OT), zoals de navigatie-, besturings- en brugsystemen.



Voordelen bij Baobab Risk Solutions:

- ✓ **Fraude-dekking:** 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.
- ✓ **Professionele ondersteuning:** In-house specialisten die helpen bij actieve security-vraagstukken en problemen.
- ✓ **Uitgebreide dekking:** Ruime dekking voor digitale gevaren.
- ✓ **Risico's in zicht:** Continue monitoring van het externe aanvalsoppervlak.



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