

Campagne Manager: Rivka Elbaz Managing Director: Saïd Laktami Graphic Design: Kiloe van Benthem Redactie: Eltjo Nieuwenhuis & Meedlawit Ogbamichael Tekst: Hugo Schrameyer, Jan Koning, Fred Pals en Michel de Ruyter Gedistribueerd met: Het Financieele Dagblad 2026 Drukkerij: RODI Rotatiedruk. Partner content in deze campagne is tot stand gekomen in samenwerking met onze klanten. Dit zijn commerciële uitingen. Dit is een commerciële uitgave. De FD-redactie heeft geen betrokkenheid bij deze productie.

Uitgegeven door
Contentway Benelux B.V.
Keizersgracht 424
NL-1016 GC Amsterdam

Tel: +31 (0)20 241 7763
Web: contentway.nl
Email: info@contentway.nl
redactie@contentway.nl

MARITIEM & OFFSHORE

 contentway
oktober 2026

**MAAKINDUSTRIE IS VAN
STRATEGISCHE WAARDE**

04

**ZEEVAART ZOEKT GROENE
KOERS**

08

**VOORSPELBAARHEID MAAKT
OFFSHORE FINANCIERBAAR**

14

Cybersecurity aan boord gaat niet alleen over data

Binnenvaartschepen worden steeds digitaal – navigatie, motormanagement, communicatieapparatuur en andere systemen zijn onderling en met de buitenwereld verbonden. Dat maakt varen efficiënter, maar het creëert ook nieuwe kwetsbaarheden. Een cyberincident kan niet alleen digitale informatie, maar alle activiteiten op het schip treffen.



André Jansma,
Maritime Data Management

“De digitale kwetsbaarheid van een binnenvaartschip zit allang niet meer alleen in een laptop of het wifi-netwerk”, zegt André Jansma van Maritime Data Management (MDM). “Steeds meer processen aan boord zijn digitaal afhankelijk. Daardoor kan een verstoring veel verder reiken dan de IT-omgeving. Zelfs tijdelijk voor onderhoud aangesloten apparatuur kan de digitale veiligheid van het schip beïnvloeden.”

Dat een schip al jarenlang probleemloos vaart, betekent volgens Jansma niet dat de risico's hetzelfde zijn gebleven. “Niet alleen het schip is in die jaren digitaal geworden, de wereld eromheen ook. Cyberdreigingen ontwikkelen zich voortdurend en aanvallers krijgen geavanceerdere middelen. Ook AI verlaagt de drempel om cyberaanvallen sneller en grootschaliger uit te voeren. Tegelijk zijn moderne binnenvaartschepen afhankelijker geworden van digitale systemen. Tien jaar zonder cyberincident zegt daarom weinig over het risico van vandaag. De techniek aan boord verandert, maar de dreiging van buitenaf verandert minstens zo snel mee. Cybersecurity moet met beide ontwikkelingen meegroeien.”

Operationele veiligheid

Bij operationele technologie (OT) wordt duidelijk waarom dat belangrijk is, aldus Jansma. “Bij een traditioneel IT-incident denk je aan gestolen gegevens, ransomware of tijdelijk onbeschikbare computersystemen. Bij OT gaat het om systemen die direct onderdeel zijn van de activiteiten. Verstoorde of gemanipuleerde navigatie- of motorsystemen kunnen direct



gevolgen hebben voor de beschikbaarheid en veiligheid van het schip.”

Cybersecurity moet volgens Jansma daarom de digitale omgeving omvatten. Daarvoor ontwikkelde Maritime Data Management MDM-PROTECT voor de binnenvaart. “Een hardware-unit monitort continu het netwerkverkeer en leert wat voor het schip normaal gedrag is. Afwijkend of verdacht verkeer wordt vervolgens gesignaleerd. Vanuit een controlekamer vindt 24/7 monitoring en indien nodig incidentrespons plaats.”

Belangrijk is dat de beveiliging aansluit op de bestaande situatie aan boord. “Geen twee schepen zijn hetzelfde; vaak functioneren oudere systemen naast nieuwe apparatuur en werken verschillende technieken en leveranciers samen. Alles vervangen is niet realistisch en meestal onnodig. Daarom brengen we eerst de digitale infrastructuur in kaart en stemmen de beveiliging daarop af.”

Leren van de praktijk

MDM-PROTECT werd in de praktijk getest op de MTS West Virginia van Wijgaart Shipping. De praktijktest liet zien hoe de oplossing functioneert op een schip dat dagelijks operationeel is. Jansma: “Op papier kun je een netwerk uitgebreid in kaart brengen, maar aan boord zie je pas echt hoe alle systemen dagelijks samenwerken. De West Virginia heeft ons laten zien hoe belangrijk het is dat een cybersecurityoplossing zich aanpast aan het schip, in plaats van andersom.”

Een belangrijk onderdeel van de test was daarom het verder verfijnen van de monitoring. “We hebben MDM-PROTECT in een operationele omgeving kunnen testen en op basis daarvan verder kunnen optimaliseren. Zo kun je nauwkeuriger bepalen welk gedrag aandacht vereist en tegelijkertijd voorkomen dat de dagelijkse werkzaamheden onnodig worden verstoord.”

“

Steeds meer processen aan boord zijn digitaal afhankelijk

Meer dan alleen techniek

Technische beveiliging is volgens hem slechts één onderdeel van digitale weerbaarheid. “Uiteindelijk zijn het de mensen aan boord die dagelijks met de apparatuur en systemen werken. Bewust omgaan met wachtwoorden, updates en externe apparatuur hoort daar bijvoorbeeld ook bij. Daarnaast moet duidelijk zijn wat iemand moet doen wanneer er iets ongebruikelijks wordt geconstateerd.”

Dat betekent volgens Jansma niet dat schippers en bemanningsleden zelf cybersecurityspecialisten moeten worden. “Een schipper moet in de eerste plaats veilig kunnen varen. Je kunt niet verwachten dat de bemanning daarnaast continu het netwerk analyseert of

cyberdreigingen beoordeelt. Daarom vinden de technische monitoring en incidentrespons bij MDM-PROTECT 24/7 vanaf de wal plaats.” De menselijke en technische kant vullen elkaar daarmee aan. “Technologie kan veel signaleren en bewaken, maar binnen een organisatie moet ook aandacht zijn voor bewustwording en duidelijke procedures. Digitale veiligheid moet uiteindelijk net zo vanzelfsprekend worden als andere vormen van veiligheid binnen de bedrijfsvoering.”

Aantoonbaar digitaal weerbaar

Die continue monitoring wordt ook belangrijker door strengere eisen rond cyberweerbaarheid en NIS2. “Organisaties moeten nadrukkelijker kijken naar hun cyberrisico's, de maatregelen die ze nemen en hoe ze omgaan met incidenten. Alleen zeggen dat je systemen beveiligd zijn, is niet voldoende. Je wilt ook kunnen laten zien wat je monitort, welke afwijkingen zijn gedetecteerd en welke maatregelen zijn genomen.”

Klanten ontvangen daarom periodieke rapportages en documentatie waarmee zij inzicht krijgen in hun cyberweerbaarheid. Jansma stelt dat veiligheid en aantoonbaarheid daardoor steeds beter op elkaar aansluiten: “Het gaat erom dat een schip digitaal weerbaar is én dat een ondernemer richting opdrachtgevers, ketenpartners of toezichthouders kan aantonen wat op het gebied van cybersecurity geregeld is.”