

## Nieuwe cyberwet: per 1 juli moet binnenvaart risico's aantoonbaar beheersen

Cyberveiligheid moet aan boord net zo belangrijk worden als de veiligheid aan dek. Dat stelt Koninklijke Binnenvaart Nederland (KBN) op basis van de nieuwe Nederlandse Cyberbeveiligingswet die op 1 juli aanstaande in werking treedt en waarop ook de binnenvaart zich moet voorbereiden. Onder de nieuwe wet vallen diverse bedrijven in de maritieme sector binnen de verplichting om een cyberrisicoanalyse te hebben en moeten zij kunnen aantonen dat zij én hun toeleveranciers cyber weerbaar zijn. Ook komt er een meldplicht voor cyber-incidenten.

Tamara BlonkRotterdam, 05 mei 2026, 07:26



Met de komst van digitale systemen zijn er ook steeds meer cyberrisico's in de binnenvaart. Foto EOC

De wet vloeit voort uit de Europese NIS2-richtlijn (2022) die Europa beter moet beschermen tegen digitale dreigingen. Die zijn ook in de binnenvaart sterk toegenomen, aangezien de bedrijfstak in hoog tempo digitaliseert. Er worden schepen op afstand bestuurd, systemen aan boord zijn steeds meer digitaal, bruggen en sluizen worden op afstand bediend, de vaarroute wordt in het online systeem ECDIS gedownload, schepen varen op TrackPilot, en met AIS-tracking worden alle schepen in kaart gebracht. Daarmee neemt de kwetsbaarheid voor cyberaanvallen toe.

Volgens brancheorganisaties in de maritieme sector, waaronder KBN, wordt cyberweerbaarheid onder de nieuwe wet een ketenverantwoordelijkheid en geen vrijblijvende keuze meer. Er komt strenger toezicht en bedrijven moeten aantonen dat ook hun toeleveranciers voldoende digitaal weerbaar zijn.

## Grootste boosdoeners

Door de digitalisering is het in principe makkelijker geworden de gang van zaken aan boord, op terminals, sluizen en bruggen van buitenaf te verstoren. Denk aan virussen, malware, data-blockers, wifi-blockers en drones die netwerken verstoren. In 2025 waren er volgens het Zuid-Koreaanse beveiligingsbedrijf Cytur **twee keer zoveel cyberaanvallen** in de maritieme sector als in 2024. Ransomware en DDOS-aanvallen waren de grootste boosdoeners als het gaat om het platleggen van systemen. Maar het gaat niet alleen om externe dreigingen, ook intern kan veel misgaan. Wie kan aan boord meekijken, systemen bedienen of informatie inzien en welke toegang hebben die mensen?

## Wachtwoord onvoldoende

Door risico's in kaart te brengen en bijvoorbeeld backup-systemen te gebruiken kan een schip cyberweerbaar worden. Digitale veiligheid aan boord begint met het instellen van een sterk wachtwoord, maar het is bijvoorbeeld ook zaak dat de software van de toeleveranciers al bij binnenkomst vrij is van virussen en malware.

*Tekst gaat verder onder foto*



Thomas Wermer van KBN roept schippers op om zich vast voor te bereiden op de nieuwe wet.  
Foto KBN

Thomas Wermer is adviseur automatisering en multimedia bij KBN. ‘We hameren er al langer op dat deze nieuwe wet eraan komt. Recentelijk hebben we als brancheorganisatie betrokken bij een pentest (een gesimuleerde, geautoriseerde cyberaanval op IT-systemen – red.) aan boord van een schip gedaan. Daar kwamen interessante dingen uit. Natuurlijk snappen we allemaal dat je moet

uitkijken voor phishing e-mails. Maar toch zitten persoonlijke en bedrijfsgegevens vaak binnen één netwerk. Het zou bijvoorbeeld beter zijn een gastennetwerk en een bedrijfsnetwerk te hebben aan boord. En de scheepsbesturing op een ander netwerk dan de gewone WiFi bijvoorbeeld. En hoever is het bereik van je WiFi-router? Probeer daar ook eens naar te kijken, zodat je de eerste bescherming zelf al regelt. En vergeet ook niet de goede en unieke wachtwoorden, met two-factor authentication waar mogelijk.’

## Samen Digitaal Veilig

Als gevolg van de nieuwe wet wordt cyberweerbaarheid onderdeel van de bevrachting en dat zal volgens Wermer wennen zijn voor veel vervoerders. ‘De eerste tijd zul je nog wel even door kunnen komen met een transitiefase, waarbij je nog niet alles hebt geïntegreerd maar wel het grootste deel. Maar we willen als KBN toch wel graag schippers aanmoedigen om zich voor te bereiden. Want het is zonde als je reizen misloopt doordat je cybersecurity niet op orde is.’

Binnenvaartondernemers kunnen zich voorbereiden via de landelijke **NIS2-scan** van de overheid en door te werken met het zogenoemde **NIS2 Supply Chain-certificaat** (voorheen NIS2 Quality Mark). Dit certificaat, ontwikkeld door Samen Digitaal Veilig, biedt MKB-bedrijven een praktisch stappenplan om hun digitale weerbaarheid aan te tonen richting klanten en ketenpartners. De kosten hiervoor bedragen, afhankelijk van het aantal werknemers, tussen de 725 en 9800 euro. Bedrijven die lid zijn van een brancheorganisatie krijgen 50% korting.

Op de website van Samen Digitaal Veilig, een initiatief van MBK-Nederland en VNO-NCW, kunnen ook **gratis webinars** worden gevolgd over de nieuwe wet. Bedrijven die onder de nieuwe wetgeving vallen kunnen door het invullen van een Estimated Risk Index (ERI) direct inzicht krijgen in hun digitale risicoprofiel en dat van hun toeleveranciers.