NIEUWE MAATREGELEN OM KANS OP AANVAL TE VERKLEINEN

SCHEPEN MOETEN CYBERSECURITY OP ORDE HEBBEN

Er zijn steeds meer cybergerelateerde incidenten, maar dankzij goede regelgeving en maatregelen zijn deze niet meer zo massaal als in 2017, toen het NonPetya-virus complete terminals platlegde. In de scheepvaart zijn sinds begin dit jaar extra maatregelen van kracht om de schade te beperken, want een schip dat getroffen wordt door een cyberaanval, veroorzaakt forse schade in de logistieke keten.

Tekst **Job Halkes**

De tijd dat alleen in films mysterieuze krachten schepen, voertuigen en bedrijven konden overnemen ligt achter ons. De afgelopen jaren is de wereld geregeld opgeschrikt door grotere en kleinere cyberaanvallen, waarbij logistieke processen in soms ernstige mate werden verstoord. Zo lagen terminals wereldwijd dagenlang stil omdat een virus was doorgedrongen tot de computers en die gijzelde, in ruil voor betalingen. Het bekendste voorbeeld is wel het NonPetya-virus, waardoor rederij Maersk enkele jaren geleden honderden miljoenen euro's schade opliep. Nieuwe en strengere regels moeten ervoor zorgen dat een degelijk virus niet meer zo ongenadig kan toeslaan of, als het toeslaat, dat de schade beperkt blijft.

Zo moet de scheepvaart sinds 1 januari voldoen aan de resolutie 'Maritime Cyber Risk Management in Safety Management Systems' van de International Maritime Organization (IMO). Daarin staat dat scheepseigenaren en -managers onder de International Safety Management Code (ISM-code) verplicht zijn om de cyberrisico's van hun schepen en organisaties in kaart te brengen, te beoordelen en zo nodig maatregelen te nemen in hun *safety management systems* (SMS).

Het NonPetya-virus gijzelde wereldwijd computers van bedrijven in 2017.

Vaarverbod

Volgens advocaten Nol van Hal en Jolien Kruit, verbonden aan advocatenkantoor Van Traa en gespecialiseerd in transport en logistiek, heeft die resolutie nogal wat gevolgen voor de rederijen en verladers die gebruikmaken van hun diensten. "Scheepseigenaren die verzuimen de nodige maatregelen te nemen ter beperking van cyberrisico's lopen, naast een cyberaanval zelf, het risico van stilliggende schepen en potentiële risico's van verzekerings- en aansprakelijkheidstechnische aard", aldus Van Hal. "Zo kan het land waar het schip geregistreerd staat het zogenoemde conformiteitsdocument, ook wel bekend als het Document of Compliance (DOC), van een scheepseigenaar of -manager intrekken bij de jaarlijkse verificatie. Het gevolg van het intrekken is dat een schip bij een controle in de eerstvolgende haven een vaarverbod krijgt opgelegd en pas verder mag varen als het gebrek is verholpen. Dat vaarverbod kan enorme financiële schade tot gevolg hebben."

Daarnaast wijst Van Hal erop dat bedrijven die lading aan boord hebben reders aansprakelijk kunnen stellen als zij niet blijken te voldoen aan de resolutie. "Een inadequate aanpak kan forse gevolgen hebben. Zo is het de vraag of het niet op orde hebben van de *cyber security* aan boord van het vervoerende schip scheepseigenaren blokkeert om een beroep te doen op verdragsrechtelijke uitsluitingen van aansprakelijkheid vanwege de onzeewaardigheid of mogelijke onzeewaardigheid van hun schepen. Ook valt niet uit te sluiten dat een schip schuldig is aan de gevolgen van een aanvaring wanneer digitale piraten de controle van het schip overnemen en het in aanvaring laten komen met een ander schip." Rederijen hebben de verplichting gekregen om bij het ontwikkelen, uitvoeren en onderhouden van hun SMS ook cyber *risks* adequaat aan te pakken. De IMO heeft in *guidelines* aandachtpunten gegeven hoe rederijen daaraan kunnen voldoen.

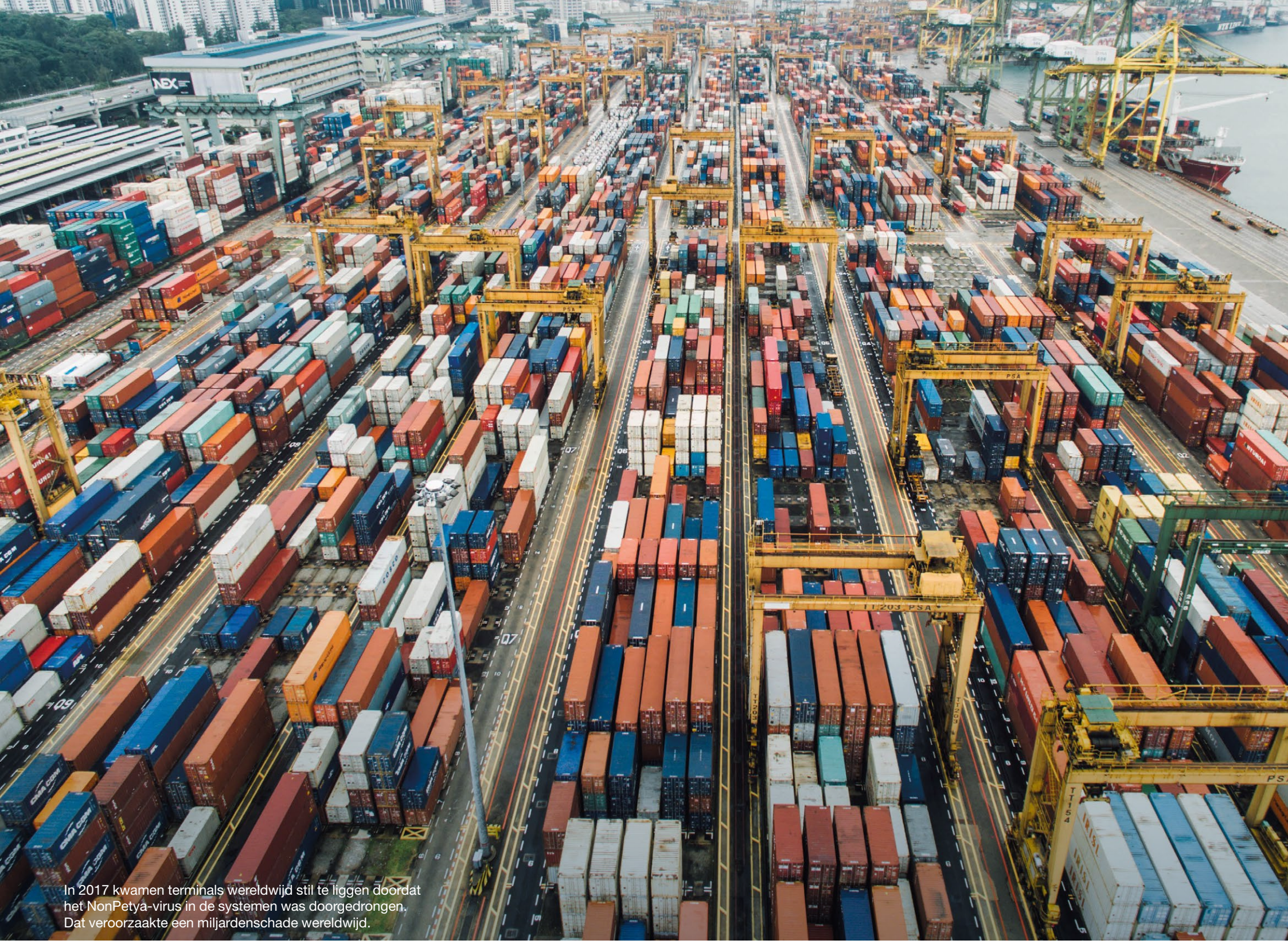
Verladers gaan volgens de twee advocaten niet direct iets van de nieuwe resolutie merken. "Dat bedoelen we in positieve zin", aldus Kruit. "De bedoeling van de resolutie is immers om cyberinbreuken te voorkomen en de gevolgen zoveel mogelijk te beperken. Als er een adequaat veiligheidsbeleid is, dat deugdelijk wordt nageleefd, zouden ladingbelanghebbenden dus geen of in ieder geval minder hinder van cyberaanvallen moeten ondervinden dan zonder de resolutie."

> "Een inadequate aanpak kan forse gevolgen hebben"

Veiligheidsplan

Landen waar het schip is geregistreerd, moeten nagaan of het veiligheidsplan van het schip op orde is. "Scheepseigenaren weten al sinds 2017 dat ze aan deze verplichtingen moeten voldoen", aldus Kruit. Verladers zelf kunnen niet altijd controleren of het veiligheidsbeleid van het vervoerende schip op orde is, omdat zij vaak contact hebben met een tussenliggende vervoerder. "Ladingbelanghebbenden kunnen er wel naar vragen, of zij kunnen in hun contracten expliciet vastleggen dat de vervoerder aan deze verplichtingen moet voldoen en daarover documentatie moet verschaffen."

"Van belang is dat het gaat om een publiekrechtelijke verplich-



In 2017 kwamen terminals wereldwijd stil te liggen doordat het NonPetya-virus in de systemen was doorgedrongen. Dat veroorzaakte een miljardenschade wereldwijd.

ting; dus van de overheid naar vervoerders", vervolgt Kruit. "Het niet nakomen van die verplichtingen kan wel privaatrechtelijke consequenties in de verhouding tussen bedrijven tot gevolg hebben. Bijvoorbeeld omdat een schip door het niet voldoen aan zijn veiligheidsverplichtingen onzeewaardig was voor en bij aanvang van een reis." Het idee om een vervoerder vooraf al aansprakelijk te stellen is een mogelijkheid als er twijfel is over een veiligheidsplan, al voegt dat volgens Kruit weinig toe. "De oplossing van een contractuele boete, voor zover vervoerders bereid zijn die overeen te komen, is dan waarschijnlijk effectiever."

Verzekeringspositie

Zelf zien Kruit en Van Hal steeds meer zaken voorbijkomen waarbij er schade is geleden door cybergerelateerde problemen. Kruit: "Dat ziet enerzijds op bewuste acties van kwaadwillenden en anderzijds op falen van software, of onkunde in de omgang daarmee. Juist door preventieve initiatieven als de Cyber Security Resolutie van de IMO wordt veel schade voorkomen."

Meer in het algemeen zijn cybersecurity, *-risks* en *-attacks* ook onderwerpen die voor de verzekeringspositie van verladers relevant kunnen zijn, aldus de twee advocaten. Van Hal: "Verladers sluiten doorgaans een (goederen)transportverzekering ter dekking van het risico van schade aan hun vervoerde goederen. De polisvoorwaarden van die verzekeringen bevatten in sommige gevallen uitsluitingen voor schades die ontstaan in verband met cyberrisks in ruime zin; denk bijvoorbeeld aan schade die ontstaat nadat de softwaresystemen aan boord van een schip worden aangevallen. Het is mogelijk de reikwijdte van dergelijke uitsluitingen te beperken bij onderhandelingen met de verzekeraar. Ook is het mogelijk een aanvullende verzekeringsdekking uit te nemen om te voorkomen dat verladers in voorkomend geval geen vergoeding van hun verzekeraars kunnen vorderen."

Toename

Senior beleidsadviseur Rogier Spoel van evofenedex herkent het beeld dat er steeds meer cybergerelateerde problemen zijn. "Er is zeker een toename van incidenten, maar dankzij maatregelen zoals die in de scheepvaart zijn die tot nu toe niet meer zo wijdverbreid als we toen bij Maersk hebben gezien. Bedrijven slagen erin om uitbraken binnen de perken te houden en ze in te dammen." Toch zijn er wel zorgen volgens Spoel. "Een cyberaanval kan een boekingsplatform verstoren en als er iets stil komt te liggen, kan dat grote schade toebrengen aan de logistieke operatie. Een andere zorg is dat belangrijke gegevens in handen komen van criminelen."
Volgens Spoel is het ook belangrijk dat reders goed communiceren over eventuele verstoringen door cyberaanvallen. "Als systemen niet bereikbaar zijn, worden bedrijven al snel ongerust. We hebben een aantal keren gezien dat er dan geruchten de ronde gaan doen over mogelijk een faillissement, terwijl het om een cyberprobleem blijkt te gaan." Dat er vanuit de IMO actie wordt ondernomen is volgens hem een goede zaak. "Dat zijn belangrijke stappen. In de toekomst wordt er nog veel meer gedigitaliseerd en dat betekent dat er een goed, veilig en gesloten systeem moet zijn."

Jolien Kruit: "Scheepseigenaren weten al sinds 2017 dat ze aan deze verplichtingen moeten voldoen."

Nol van Hal: "Een vaarverbod kan enorme financiële schade tot gevolg hebben."

Rogier Spoel: "Een cyberaanval kan een boekingsplatform verstoren."