Port of Rotterdam

Ministerie van Veiligheid en Justitie
T.a.v. de heer dr. K.H.D.M. Dijkhoff
Turfmarkt 147
2511 DP DEN HAAG

Datum 14 juli 2017
Ons kenmerk HBR-1414674
Aantal bijlagen –
Contactpersoon
Telefoon
E-mail

Onderwerp reactie internetconsultatie Cybersecuritywet/ implementatie NIB-richtlijn

Geachte heer Dijkhoff,

Cyber Resilience staat al ruim een jaar hoog op de agenda in de haven van Rotterdam. Des te meer betreur ik het dat op 27 juni jongstleden APM Terminals in Rotterdam is geraakt door de Petya ransomware. Voor mij en de programmapartners van Ferm[1] een aanmoediging om onze inspanningen op het gebied van cybersecurity in de Rotterdamse haven onverminderd door te zetten. Maar ook om te beseffen dat een bepaalde vrijblijvendheid omtrent het delen van informatie niet meer mag bestaan. Het ondermijnt de mogelijkheden en informatiepositie om tijdig passende repressieve maatregelen te nemen in het havengebied en daarmee een veilige afwikkeling van al het verkeer in de haven. Daarom wil ik versneld inzetten op een meldplicht cybersecurity voor -te beginnen bij- de zogenaamde ISPS bedrijven. De mogelijkheden hiertoe zijn er en worden momenteel nader verkend.

Met betrekking tot de door mij voorgelegde vragen in de internetconsultatie Besluit meldplicht cybersecurity van 16 mei jl., ik ben hierover in gesprek met het Ministerie van Infrastructuur & Milieu en het NCSC. Ik heb het volste vertrouwen dat we hier tijdig de juiste richting en antwoorden in vinden.

Om op de internetconsultatie van de voorliggende Cybersecuritywet (Csw) te komen, wil ik u graag het volgende ter overweging meegeven:

- Ik ondersteun uw keuze om de Wet gegevensverwerking en meldplicht cybersecurity beleidsneutraal te incorporeren in de Csw en zo de wetgeving rondom cybersecurity helder te houden.

[1] Voor meer informatie: www.ferm-rotterdam.nl

Port of Rotterdam

Datum 14 juli 2017
Ons kenmerk HBR-1414674

- Heeft u in het kader van de voorgestelde minimumharmonisatie, bewust gekozen dat Havenfaciliteiten wel in de NIB-richtlijn worden genoemd, maar niet in de Nederlandse implementatie in de Csw?
- Worden de globale en specifieke beveiligingseisen waar de aanbieder van de essentiële dienst aan moet voldoen, door het Ministerie van Infrastructuur & Milieu verder uitgewerkt in een sectorale amvb, alsmede de wijze van toezicht van de bevoegde autoriteit?
- Kwetsbaarheden in hard- en software kunnen invloed hebben op de veiligheid van de netwerken van aanbieders van essentiële diensten, terwijl er op dit moment geen passende waarborgen zijn voor de veiligheid van deze producten. Ik pleit daarom voor de ontwikkeling van kwaliteitseisen voor hard- en software op Europees niveau.
- Er is gekozen voor sectoraal toezicht op de Csw. Dat betekent in het geval van bijvoorbeeld Portbase B.V., dat deze wordt geconfronteerd met verschillende toezichthouders. Ik stel daarom een door het Ministerie van Veiligheid & Justitie geharmoniseerde aanpak voor, om de toezichtslasten minimaal te laten zijn.

Ik neem bovenstaande onderwerpen graag mee in de lopende gesprekken met het Ministerie van Infrastructuur & Milieu en het NCSC.

Met vriendelijke groet,

Havenmeester van Rotterdam
Rijkshavenmeester regio Rijnmond

In afschrift aan:
- de Minister van Infrastructuur & Milieu
- Hoofd Nationaal Cyber Security Centrum