Port of Rotterdam

HAVEN CYBER MELD PUNT

Beleidsdocument

INHOUDSOPGAVE

1. INLEIDING

De Rotterdamse haven is in sterke mate afhankelijk van informatie technologie (IT) voor de veilige en vlotte afwikkeling van het scheepvaart- en wegverkeer en de overige modaliteiten. Digitalisering kan leiden tot IT verstoringen in het havengebied en zorgt daarmee voor risico's voor de veiligheid en continuïteit in de Rotterdamse haven. Digitale veiligheid en continuïteit staan dan ook hoog op de agenda van de Havenmeester en de maritieme sector[1].

De veiligheidseffecten van een IT verstoring hoeven zich niet te beperken tot het direct getroffen bedrijf. Zo kunnen verstoringen ook neveneffecten hebben op indirect betrokken partijen of processen. Dit kan zorgen voor problemen elders in de keten, bijvoorbeeld in de afhandeling van het weg- en scheepvaartverkeer in het havengebied en in de regio. Wanneer deze problemen niet adequaat worden voorkomen of opgelost kan de veiligheid en continuïteit in de haven in het geding komen.

Verschillende bedrijven in de haven zijn geconfronteerd met onopzettelijke en opzettelijke IT verstoringen die tot een tijdelijke sluiting van de bedrijven hebben geleid. Deze verstoringen hadden directe gevolgen voor het havengebied, waardoor de Havenmeester genoodzaakt was om maatregelen te nemen die er bijvoorbeeld voor zorgen dat het scheepvaartverkeer veilig kan worden afgehandeld.

Naast het in geding komen van de veilige afhandeling van het verkeer kan uitval van IT ook gevolgen hebben voor de veiligheidsmaatregelen in het kader van de Havenbeveiligingswet. Zo kan een verstoring ertoe leiden dat de toegang tot de havenfaciliteit niet meer kan worden gecontroleerd met behulp van een geautomatiseerd toegangscontrole systeem of dat de camerabewaking tijdelijk uitvalt.

[1] International Maritime Organization (IMO) heeft ten aanzien van cyber risk management zowel een Resolutie (nr. MSC.428[98], 16 juni 2017) als Guidelines (nr. MSC-FAL.1/Circ.3, 5 juli 2017) aangenomen.

1.1 HAVEN CYBERMELDPUNT OP HET HAVEN COÖRDINATIE CENTRUM

De Rotterdamse haven is door het Rijk aangewezen als onderdeel van de Nederlandse vitale infrastructuur. Hierdoor heeft het Havenbedrijf Rotterdam, in het bijzonder de Havenmeester, de plicht om de veiligheid en continuïteit van de haven te borgen. De Havenmeester opent daarom op 11 juni 2018 een meldpunt voor bedrijven in de haven zodat zij melding kunnen maken van IT verstoringen die impact hebben op hun bedrijfsvoering en daarmee mogelijk op de veiligheid in het Havengebied. Het melden van dergelijke IT verstoringen is verplicht voor alle bedrijven die moeten voldoen aan de Havenbeveiligingswet[2]. Overige bedrijven worden nadrukkelijk gevraagd vrijwillig te melden. Het meldpunt wordt ingericht bij het Haven Coördinatie Centrum (HCC) van de Divisie Havenmeester (DHMR) en zal bekend staan als het Haven Cybermeldpunt.

Op basis van de melding kan de Havenmeester maatregelen nemen die bijdragen aan de veiligheid in het havengebied. De Havenmeester werkt hiervoor samen met de veiligheidspartners in de haven en regio.

Het doel van het Haven Cybermeldpunt is bijdragen aan de veiligheid en continuïteit van de Rotterdamse haven tijdens en na IT verstoringen.

1.2 OPBOUW BELEIDSDOCUMENT

Dit beleidsdocument is opgesteld om het Haven Cybermeldpunt en de onderliggende grondslagen aan de havengemeenschap te introduceren. Het document begint met een uitleg over IT verstoringen en legt uit voor wie de meldplicht geldt en in welke scenario's een melding verplicht en/of gewenst is. Vervolgens volgt een uitleg over het maken van een melding en welke acties bij het Haven Cybermeldpunt en de meldende partij liggen. Tot slot licht het document de wettelijke grondslagen toe waarop de meldplicht is gebaseerd en wordt de handhaving van de meldplicht beschreven.

[2] Havenbeveiligingswet in te zien via http://wetten.overheid.nl/BWBR0016991/2010-10-01

2. WAT IS EEN IT VERSTORING?

Een melding dient alleen gemaakt te worden wanneer de verstoring gevolgen heeft voor de veiligheid en continuïteit van de bedrijfsvoering van de meldende partij of mogelijk op de veiligheid en continuïteit van de haven. De Havenmeester maakt onderscheid tussen twee typen IT verstoringen: een onopzettelijke IT verstoring en een opzettelijke IT verstoring.

- Een onopzettelijke IT verstoring is een veiligheidsincident in de digitale infrastructuur van een bedrijf waardoor de te verwachten veiligheid en continuïteit van de bedrijfsvoering in het geding is gekomen of in het geding komt. Bijvoorbeeld een onopzettelijke en onverwachte uitval van systemen naar aanleiding van een aanpassing in de digitale infrastructuur van het bedrijf.

  De Havenmeester zal bij een dergelijke verstoring de melding aannemen en waar nodig en in overleg met de meldende partij maatregelen nemen voor de veiligheid in de haven. Daarnaast is het mogelijk dat de Havenmeester de melding communiceert aan de relevante (veiligheids)partners.

  Let op: een onopzettelijke verstoring kan later een opzettelijke verstoring (cyberaanval) blijken.

- Een opzettelijke IT verstoring is in de regel een cyberaanval: een (al dan niet gerichte) aanval om de digitale infrastructuur van het bedrijf binnen te dringen, te beschadigen of buiten werking te stellen. In het geval van een opzettelijke verstoring is er een bewuste poging om de systemen ongeautoriseerd te benaderen. Dit gebeurt meestal door buitenstaanders (concurrenten, criminelen en/of terroristen). Indien het een cyberaanval betreft wordt de getroffen partij dringend geadviseerd om naast de melding aan het Haven Cybermeldpunt ook aangifte te doen bij de Politie.

  De Havenmeester zal bij een dergelijke verstoring in overleg met de meldende partij maatregelen nemen voor de veiligheid in de haven. Wanneer het een cyberaanval betreft zal de Havenmeester, afhankelijk van het type en de impact, communiceren met het Nationaal Cyber Security Centrum (NCSC). Eventuele communicatie naar de overige bedrijven in de haven zal worden afgestemd met de meldende partij.

3. WANNEER GELDT DE MELDPLICHT?

De meldplicht geldt voor de bedrijven die moeten voldoen aan de Havenbeveiligingswet (ISPS-plichtige bedrijven). Daarnaast geldt de meldplicht voor Portbase en de nautische dienstverleners[3]. Alle overige bedrijven worden aangemoedigd om een vrijwillige melding te doen. Een directe melding van de IT verstoring is verplicht wanneer voldaan wordt aan de volgende voorwaarden:

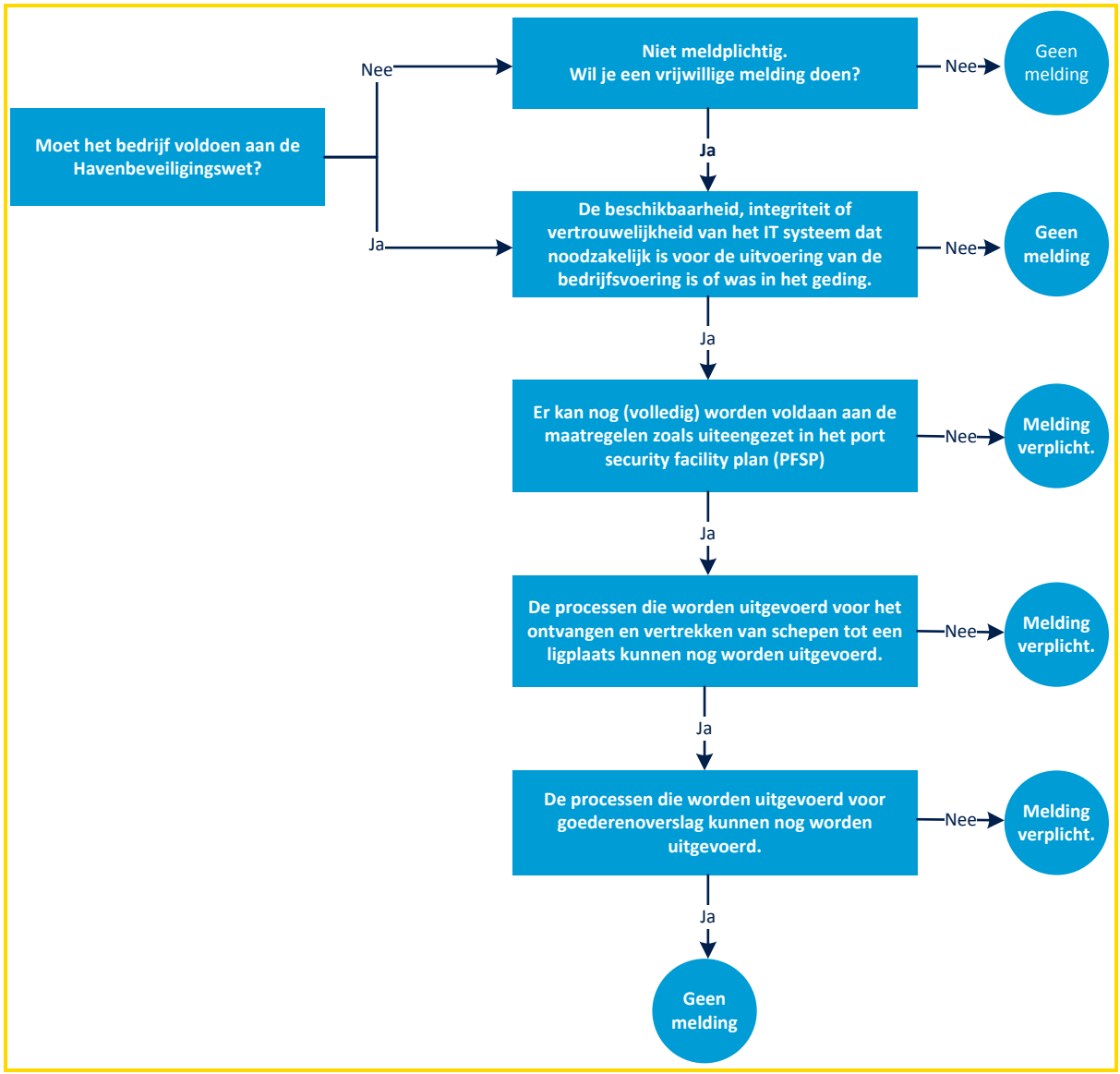
1) Het bedrijf moet voldoen aan de Havenbeveiligingswet of is in het bezit van een havenbeveiligingscertificaat of het bedrijf is een nautisch dienstverlener.

2) De beschikbaarheid, integriteit of vertrouwelijkheid van het IT systeem dat noodzakelijk is voor de uitvoering van de bedrijfsvoering is of was in het geding.

3) Daarnaast dient de verstoring één (of meer) van de drie onderstaande gevolgen teweeg brengen.
   a) Het is niet meer mogelijk om (een gedeelte van) de maatregelen uit het port facility security plan uit te voeren.
      en/of
   b) Onderbreking van processen voor het ontvangen en vertrekken van (zee)schepen die mogelijk bedreigend is voor de veiligheid van het bedrijf.
      en/of
   c) Onderbreking van de processen rondom goederenoverslag die mogelijk bedreigend is voor de veiligheid van het bedrijf.

Wanneer géén van de gevolgen als geformuleerd onder punt drie van toepassing is, is het melden van een verstoring niet noodzakelijk. Het onderstaande overzicht geeft aan wanneer een melding verplicht is.

[3] KRVE Koninklijke Roeiers Vereeniging Eendracht, het Nederlands Loodswezen en de sleepdiensten.



Wanneer het een opzettelijke verstoring betreft (bv. een cyberaanval) maar dit geen gevolgen heeft zoals geformuleerd onder punt 3, is het nog altijd wenselijk om vrijwillig te melden. De Havenmeester kan door de informatie uit de melding mogelijk een handelingsperspectief bieden aan andere bedrijven zodat zij hun digitale infrastructuur kunnen beschermen tegen een cyberaanval. De Havenmeester kan door de melding tevens een inschatting maken of het probleem breder speelt of kan gaan spelen en of hij maatregelen moet nemen voor de veiligheid en continuïteit in het havengebied.

4. HOE MOET EEN MELDING GEMAAKT WORDEN?

Meldingen dienen telefonisch gemaakt te worden bij het Haven Cybermeldpunt op +31 (0)10 252 1005. De HCC Duty Officer zal de melding opnemen en het uitvraagprotocol[4] (zie bijlage 1) toepassen, waarbij (voor zover bekend) in ieder geval de volgende informatie dient te worden verstrekt:

- Details over het getroffen bedrijf;
- Omschrijving van de verstoring;
- Details over de (veiligheids)impact op de bedrijfsvoering en eventuele neveneffecten;
- Informatie over de impact van de verstoring op de verkeersafhandeling en de algehele veiligheid;
- De contactgegevens van de functionaris die verantwoordelijk is voor de melding en contactpersonen voor de Havenmeester, Havenbedrijf Rotterdam afdeling Assetmanagement en de Havenbedrijf Rotterdam Information Security Officer.

Meldingen dienen zo spoedig mogelijk te worden gedaan bij het Haven Cybermeldpunt. De initiële melding kan beknopt zijn: de voorkeur gaat uit naar een snelle melding die zo nodig later wordt aangevuld met bovenstaande informatie, dan een uitvoerige melding die op zich laat wachten. Hoe eerder de melding binnen is, hoe groter de kans dat de Havenmeester vroegtijdig maatregelen kan inzetten om (veiligheids)gevolgen verderop in de keten te beperken.

De Havenmeester adviseert de bedrijven die vallen onder de meldplicht het melden van IT verstoringen in het reguliere (IT) incidenten proces op te nemen.

[4] Het uitvraagprotocol is in bijlage 1 aan dit beleidsdocument toegevoegd.

5. WAT DOET HET HAVEN CYBERMELDPUNT MET DE MELDING?

Door het melden van de IT verstoring kan de Havenmeester een inschatting maken van de impact op het havenlogistiek proces. Dit is van belang gezien een verstoring verdergaande gevolgen kan hebben op het scheepvaart- en wegverkeer en de overige modaliteiten. Het belang van de melding ligt daarmee niet alleen bij de meldende partij maar juist ook bij de overige bedrijven in de haven.

De Havenmeester en het Havenbedrijf Rotterdam bieden nadrukkelijk géén IT ondersteuning aan en richten zich niet op het oplossen van de IT verstoring. De volgende actiepunten kunt u wél verwachten van de Havenmeester en het Havenbedrijf:

- Bepalen of er (aanvullende) maatregelen nodig zijn ter ondersteuning van de veilige afhandeling van het scheepvaartverkeer. Hierbij valt te denken aan het inzetten van extra patrouilles of het herprioriteren van de scheepvaart.
- Bepalen in overleg met partners of er (aanvullende) maatregelen nodig zijn ter ondersteuning van de veilige afhandeling van het wegverkeer en overige logistiek. Hierbij valt te denken aan het instellen van een truckbufferplan en meldingen om het verkeer om te leiden.
- Bepalen of het Haven Crisisteam onder voorzitterschap van de Havenmeester bijeen moet komen. Als een IT verstoring gevolgen heeft voor meerdere partijen in de haven en overleg over de logistieke en nautische gevolgen en maatregelen nodig is, wordt het Haven Crisisteam geactiveerd. Het Haven Crisisteam bespreekt in de breedte de impact op de Haven en alle modaliteiten. Afhankelijk van de samenstelling kan het Haven Crisisteam (aanvullende) maatregelen nemen ter ondersteuning van de veiligheid in de haven en in de regio.
- Het getroffen bedrijf kan worden uitgenodigd om deel te nemen aan het crisisteam.
- Waar nodig zal de Havenmeester derden informeren over de verstoring en met name de gevolgen van het incident. De Havenmeester kan doormelden aan de volgende partners:
    - De nautisch dienstverleners: ter bevordering van de veiligheid op het water.
    - De Zeehavenpolitie: ter bevordering van de veiligheid in het havengebied.
    - De Veiligheidsregio Rotterdam-Rijnmond: ter bevordering van de veiligheid in het havengebied en de regio.
    - Het Nationaal Cyber Security Centrum: om te voldoen aan de wettelijke meldplicht van de Havenmeester[5].
    - Overige relevante stakeholders[6]: ter bevordering van de weerbaarheid in het havengebied.

De Havenmeester is er zich van bewust dan een melding van een IT verstoring gevoelige informatie kan bevatten. Het delen van informatie met bovengenoemde instanties vindt plaats daar waar dat noodzakelijk is om de veiligheid in het havengebied te bevorderen. Het informeren van de overige (private) havenfaciliteiten zal altijd worden afgestemd met de meldende partij en wanneer gewenst geanonimiseerd plaatsvinden.

[5] Meldplicht inzake de Wet Gegevensverwerking en Meldplicht Cybersecurity (WGMC). Deze wet wordt naar verwachting in 2018 vervangen door de Wet beveiliging netwerk- en informatiesystemen waarin de meldplicht voor de Havenmeester wordt overgenomen.

[6] Bijvoorbeeld: Deltalinqs, DCMR Milieudienst Rijnmond, Rijkswaterstaat, Gemeente Rotterdam, etc.

6. WAT DOET DE MELDENDE PARTIJ?

De meldende partij blijft te allen tijde verantwoordelijk voor het oplossen van de IT verstoring. Daarnaast blijft de meldende partij verantwoordelijk voor de eigen digitale infrastructuur en voor de veiligheid op het eigen terrein. In het kader van die verantwoordelijkheden is het ook mogelijk dat het getroffen bedrijf een melding moet maken bij andere autoriteiten zoals de Politie of de Autoriteit Persoonsgegevens.

De Havenmeester vraagt de meldende partij de volgende acties te ondernemen:

- Melden van de IT verstoring en verstrekken van gevraagde informatie.
- Indien nodig: de Havenmeester vragen maatregelen te nemen ter ondersteuning van de veilige afhandeling van het scheepvaart- en wegverkeer, waarbij het meldende bedrijf een inschatting van de verwachte impact op de verkeersafhandeling geeft.
- Contactpersoon (of contactpersonen) aanstellen voor de volgende onderwerpen:
    - Coördinatie over eventueel te nemen maatregelen waterzijde.
    - Coördinatie over eventueel te nemen maatregelen landzijde.
    - Verdere technische en informatiebeveiligingsinformatie.
- Eventueel deelnemen aan het Haven Crisis Team op uitnodiging van de Havenmeester.
- Afhankelijk van de prognose en het verloop van de IT verstoring het meldpunt voorzien van tussentijdse updates.
- Afmelden van de verstoring wanneer de bedrijfsvoering hervat is.

7. GRONDSLAGEN MELDPLICHT EN MELDPUNT

7.1 GRONDSLAGEN MELDPLICHT

De melding van een IT verstoring is verplicht voor ISPS-plichtige bedrijven en voor Portbase en de nautische dienstverleners[7].

Op grond van EU Verordening 725/2004 moeten ISPS-plichtige bedrijven veiligheidsincidenten melden.[8] In de havens van Rotterdam en Drechtsteden houdt deze procedure in dat bedrijven (fysieke) veiligheidsincidenten dienen te melden bij de Zeehavenpolitie.

Gelet op het doel van de EU Verordening (verbetering van de beveiliging van schepen en havenfaciliteiten tegen het gevaar van opzettelijke ongeoorloofde acties[9]) valt onder het begrip "veiligheidsincident" zowel fysieke als digitale veiligheid. Deze zijn (zeker tegenwoordig) immers niet van elkaar te scheiden. De EU Verordening van 2004 benoemt reeds het belang van computersystemen en –netwerken[10] en de IMO heeft hier in eerder genoemde resolutie en guidelines in 2017 nogmaals aandacht aan geschonken.

Het voorgaande houdt in dat cyberincidenten die bedreigend zijn voor de havenfaciliteit, schepen dan wel het schip/haven raakvlak, op grond van het bepaalde in de Verordening gemeld moeten worden. Nieuw is dat deze incidenten dan niet, zoals andere veiligheidsincidenten, aan de Zeehavenpolitie moeten worden gemeld, maar aan het Haven Cybermeldpunt.

Tot slot, de meldplicht voor Portbase geldt op basis van de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) en de aankomende Wet beveiliging netwerk- en informatiesystemen. De bedrijven die onder de meldplicht vallen hebben een spilfunctie in de Rotterdamse haven en zijn onmisbaar voor de veiligheid en continuïteit van de (scheepvaart)verkeersafwikkeling. In het kader van de Wgmc zijn of worden individuele afspraken gemaakt met Portbase over het melden van IT incidenten. Ook worden individuele afspraken gemaakt met de nautische dienstverleners.

[7] KRVE Koninklijke Roeiers Vereeniging Eendracht, Het Nederlands Loodswezen en de sleepdiensten.

[8] Veiligheidsincident: iedere verdachte handeling of omstandigheid die bedreigend is voor de veiligheid van een schip, met inbegrip van de veiligheid van een booreenheid, een hogesnelheidsvaartuig, een havenfaciliteit, een schip/haven raakvlak of een schip-tot-schip-activiteit (art. 1.13 van voorschrift 1 van bijlage 1 van EU Verordening 725/2004.)

[9] art. 1 van EU Verordening 725/2004

[10] Vb. artt. 15.3, 15.7 en 15.16 van deel B van Bijlage III van de Verordening

7.2. GRONDSLAGEN HAVEN CYBERMELDPUNT BIJ HET HCC

Het besluit om het Haven Cybermeldpunt bij het HCC van de Divisie Havenmeester te beleggen is afgestemd met de Zeehavenpolitie en de Veiligheidsregio Rotterdam-Rijnmond (VRR) en vloeit voort uit de wettelijke verantwoordelijkheden die de Havenmeester draagt. Daarnaast is het de Havenmeester die in staat is om direct acties te ondernemen om een bijdrage te leveren aan de veiligheid en continuïteit van het haven logistiek proces. De volgende verantwoordelijkheden liggen ten grondslag aan het meldpunt op het HCC:

1. Havenbeveiligingswet, Port Security Officer en de WGMC
   De Havenmeester is aangesteld als Port Security Officer die er voor zorgt dat de Havenbeveiligingswet wordt nageleefd. Naleving van de Havenbeveiligingswet wordt gecontroleerd door het uitvoeren van inspecties. In de rol als Port Security Officer is de Havenmeester namens de Burgemeester de autoriteit voor de veiligheid in de haven.

   De Burgemeester en in mandaat de Havenmeester zijn onder de Havenbeveiligingswet verplicht om contactinformatie te verstrekken voor het melden van (IT) verstoringen die vallen onder de Havenbeveiligingswet. Door het instellen van het Haven Cybermeldpunt creëert de Havenmeester een specifiek meldpunt voor IT verstoringen. De Havenmeester kan naar aanleiding van de melding vervolgacties coördineren die bijdragen aan de veiligheid van het verkeer in de haven.

   Daarnaast heeft het Havenbedrijf Rotterdam en in het bijzonder de Havenmeester in het kader van de Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) een meldplicht aan het Nationaal Cyber Security Centrum (NCSC) wanneer IT verstoringen een ontwrichtend effect op de maatschappij hebben. Voorts is het van belang dat de Havenmeester kennis heeft van de IT verstoringen in het havengebied en in staat is een inschatting te maken van een eventueel (ontwrichtend) effect op de maatschappij. De Wgmc wordt in 2018 vervangen door de Wet beveiliging netwerk- en informatiesystemen waar deze meldplicht ook in wordt opgenomen.

2. Veilig en geordend scheepvaartverkeer
   De Havenmeester is verantwoordelijk voor een veilige, vlotte, schone en beveiligde afwikkeling van de scheepvaart in de haven van Rotterdam. Daarmee heeft de Havenmeester een verantwoordelijkheid om daar waar verstoringen plaats vinden de expertise in te zetten om de veilige en geordende afhandeling van het verkeer (in het bijzonder scheepvaartverkeer) te ondersteunen[11].

   Daar waar IT verstoringen een impact hebben op de bedrijfsvoering aan de waterzijde van de meldende partij zal de Havenmeester indien nodig actie ondernemen. Hierbij valt te denken aan het inzetten van extra patrouilles, het herprioriteren van de scheepvaart en het informeren van de nautische dienstverleners.

[11] Havenmeester-convenant Rotterdam in te zien via https://zoek.officielebekendmakingen.nl/stcrt-2004-2-p7-SC63196.html

3. Veilig en geordend wegverkeer
   Het Havenbedrijf Rotterdam beheert een groot deel van de infrastructuur in het havengebied en werkt nauw samen met Rijkswaterstaat om een bijdrage te leveren aan de veiligheid en continuïteit van het wegverkeer.

   Daar waar IT verstoringen een impact hebben op de bedrijfsvoering aan de landzijde van de melder zal de Havenmeester de informatie doormelden aan de Asset Manager van het Havenbedrijf. Dit stelt de Asset Manager in staat om indien nodig actie te ondernemen. Hierbij valt te denken aan het instellen van een truckbufferplan ter voorkoming van opstoppingen en coördinatie met Rijkswaterstaat over de bewegwijzering.

4. Veilig en geordend verloop van de overige modaliteiten (logistiek)
   Naast het veilig en geordend verwerken van het scheepvaart- en wegverkeer is er in de Rotterdamse haven spoor- en ondergrondse infrastructuur aanwezig. Deze modaliteiten hebben ook afhankelijkheden met andere bedrijven en informatie technologie. IT verstoringen kunnen tot een tijdelijke uitval of verstopping in de deze modaliteiten leiden, wat gevolgen kan hebben voor de veiligheid in de haven. De Havenmeester kan het Haven Crisisteam bijeenroepen om te bepalen of er (aanvullende) maatregelen nodig zijn om het veilig en geordend verloop van de overige modaliteiten te ondersteunen.

8. HANDHAVING

De meldplicht is primair gericht op het anticiperen op de mogelijk bredere veiligheidseffecten van een IT verstoring. Vooral door andere onderdelen van de haven alsook andere bedrijven in overleg met de melder te waarschuwen en handelingsperspectief te bieden. Het doen van een melding draagt daarmee bij aan de veiligheid en de continuïteit van de haven en de bedrijfseconomische activiteiten in het havengebied.

Wanneer een meldingsplichtige partij verzuimt melding te doen van IT verstoringen zal de Port Security Officer met het betreffende bedrijf in contact treden. Daarnaast zal de meldplicht onderdeel zijn van de (jaarlijkse) evaluatie in het kader van de Havenbeveiligingswet. Tot slot kan de Havenmeester – indien een bedrijf blijft verzuimen een IT verstoring te melden, een last onder dwangsom opleggen.

9. TOT SLOT

De meldplicht draagt bij aan het creëren van een cultuur in de Rotterdamse Haven waarin het gezamenlijk werken aan digitale veiligheid centraal staat. Om een dergelijke cultuur te bevorderen is het bij het doen van de melding van belang dat deze in vertrouwen gedaan kan worden. Het Havenbedrijf Rotterdam en de Havenmeester zijn zich zeer bewust van de gevoeligheid van de te delen informatie en zal hier samen met de publieke partners zorgvuldig mee omgaan.

De wetgeving en verplichtingen op het gebied van digitale veiligheid zijn sterk in ontwikkeling. Nieuwe wet- en regelgeving richten zich voornamelijk op het waarborgen van de veiligheid en continuïteit van IT en privacy van betrokkenen. In dat kader is er onder andere door de IMO veel aandacht voor het onderwerp en zal er vanuit verschillende organisaties meer richtlijnen beschikbaar komen met betrekking tot cyber risk management. Deze ontwikkeling zal zich in de komende jaren ook uiten in de vereisten voor het port facility security plan. Gezien de ontwikkelingen zien het Havenbedrijf, de Havenmeester, Deltalinqs, de Gemeente en de Politie ruimte weggelegd voor samenwerking tussen alle partijen in de haven: met samenwerking en informatiedeling kunnen de vraagstukken op het gebied van veiligheid en continuïteit op het digitale vlak efficiënt en effectief opgepakt worden.

BIJLAGE 1 - UITVRAAGPROTOCOL HAVEN CYBERMELDPUNT

1. Bedrijf:
    a. Wat is uw naam en functie?
    b. Wat is de bedrijfsnaam?
    c. Wat is het adres?
    d. Wat is het type bedrijf?[12]

2. Impact van de IT verstoring op het bedrijf van de meldende partij:
    a. Wat voor gevolgen heeft de IT verstoring op uw bedrijf?
    b. Hoe laat merkte u voor het eerst iets van de IT verstoring?
    c. Is bekend wat de oorzaak is van de IT verstoring?
    d. Welke maatregelen heeft u genomen?
    e. Wanneer verwacht u dat het probleem verholpen is?

3. Havenbeveiligingswet/ISPS:
    a. Valt het bedrijf onder de Havenbeveiligingswet/ISPS?
        - Indien ‘ja’ door naar vraag 3b.
        - Indien ‘nee’ door naar vraag 4
    b. Voldoet u nog aan het havenfaciliteit beveiligingsplan?
        - Indien ‘ja’ door naar vraag 4.
        - Indien ‘nee’ door naar vraag 3c.
    c. Welke maatregelen kunt u niet meer uitvoeren?

4. Veiligheid van het verkeer
    a. Heeft de IT verstoring gevolgen voor de verkeersafwikkeling aan de land- of waterzijde?
    b. Indien ja: welke problemen verwacht u met de verkeersafwikkeling?[13]

5. De contactgegevens van (dit kan één en dezelfde persoon zijn):
    a. Wat zijn uw contactgegevens?
    b. Wie kunnen we spreken over de afhandeling van het scheepvaartverkeer?
    c. Wie kunnen we spreken over afhandeling van het wegverkeer?
    d. Wie kunnen we spreken over de IT en IT beveiliging?

[12] O.a. containers, droge bulk, natte bulk, biobased, LNG, breakbulk, raffinage, chemie, energie of offshore.

[13] De verwachte verkeersimpact is belangrijk om in te schatten of er maatregelen moeten worden genomen door HbR om het verkeer op het water en land in goede banen te sturen.

Cybermeldpunt Haven Coördinatie Centrum
www.portofrotterdam.com/nl/scheepvaart/port-security
+31 (0)10 – 252 1005

Port of Rotterdam