Port of Rotterdam

HAVEN CYBER MELD PUNT

Beleidsdocument

CONTENTS

1. INTRODUCTION

The Port of Rotterdam is highly dependent on information technology (IT) for the secure and smooth handling of shipping traffic, road traffic and other modalities. Digitisation can result in IT disruptions in the port area, which consequently results in risks for security and continuity in the Port of Rotterdam. Digital security and continuity are therefore a high priority for the Harbour Master and the maritime sector[1].

The security effects of an IT disruption are not necessarily limited to the immediately affected company. Such disruptions can also have secondary effects on indirectly involved parties or processes and can result in problems elsewhere in the chain, such as handling road and shipping traffic in the port area and region. If these problems are not prevented or resolved effectively, port security and continuity could be jeopardised.

Various companies in the port have been confronted with unintentional or intentional IT disruptions that have resulted in a temporary company shutdown. These disruptions had direct consequences for the port area, with the Harbour Master being forced to take measures, for instance to ensure the secure handling of shipping traffic.

As well as jeopardising the secure handling of traffic, IT disruptions can also have consequences for security measures in the context of the Port Security Act. For instance, a disruption could result in it no longer being possible to control access to the port facility using an automated access control system, or that the camera surveillance becomes temporarily unavailable.

[1] With respect to cyber risk management, the International Maritime Organization (IMO) has adopted both a Resolution (no. MSC.428[98], 16 June 2017) and Guidelines (no. MSC-FAL.1/Circ.3, 5 July 2017).

1.1 PORT CYBER NOTIFICATION DESK AT THE HARBOUR COORDINATION CENTER

The Port of Rotterdam is designated by the government as being part of the vital infrastructure of the Netherlands. This means that the Port of Rotterdam Authority, and particularly the Harbour Master, has a duty to safeguard port security and continuity. That is why the Harbour Master established a notification desk for companies in the port on 11 June 2018, so that they can report IT disruptions that impact their commercial operations and could potentially also impact Port area security. The reporting of such IT disruptions is mandatory for all those companies that must comply with the Port Security Act.[2] Other companies are requested to report such disruptions voluntarily. The notification desk was established by the Harbour Coordination Center (HCC) of the Harbour Master's Division (DHMR) and is known as the Port Cyber Notification Desk.

The Harbour Master can use the reports to take measures that contribute to port area security. The Harbour Master cooperates with security partners in the port and region for this.

The objective of the Port Cyber Notification Desk is to contribute to security and continuity in the Port of Rotterdam during and following IT disruptions.

1.2 POLICY DOCUMENT STRUCTURE

This policy document was formulated to introduce the Port Cyber Notification Desk and its underlying principles to the port community. The document starts with an explanation about IT disruptions and explains which companies have a mandatory reporting obligation and in which scenarios a report is mandatory and/or desired. This is followed by an explanation of how to submit a report and the actions to be taken by the Port Cyber Notification Desk and the reporting party. Finally, the document identifies the legislative principles on which the mandatory reporting obligation is based and describes the enforcement of the reporting obligation.

[2] View the Port Security Act via http://wetten.overheid.nl/BWBR0016991/2010-10-01

2. WHAT IS AN IT DISRUPTION?

A report should only be made when the disruption has consequences for the security and continuity of the reporting party's commercial operations or potentially for port security and continuity. The Harbour Master distinguishes two types of IT disruptions: an unintentional IT disruption and an intentional IT disruption.

- An unintentional IT disruption is a security incident in a company's digital infrastructure in which it is expected that the security and continuity of commercial operations have been or will be jeopardised. For example, an unintentional and unexpected outage of systems as a result of a company making changes to its digital infrastructure.

  For such a disruption, the Harbour Master will accept the report and, where necessary and in consultation with the reporting party, take measures to ensure port security. It is also possible that the Harbour Master will communicate the report to relevant security and other partners.

  Please note: an unintentional disruption may later appear to be an intentional disruption (cyber-attack).

- An intentional IT disruption is generally a cyber-attack: a targeted or untargeted attack to penetrate, damage or shut down the company's digital infrastructure. In intentional disruptions, a deliberate and unauthorised attempt has been made to access the systems. This is usually carried out by outsiders (competitors, criminals and/or terrorists). If a cyber-attack is involved, the affected party is urgently advised to notify the police as well as reporting to the Port Cyber Notification Desk.

  For such a disruption, the Harbour Master will consult with the reporting party regarding taking measures to safeguard port security. If there is a cyber-attack, depending on the type and impact, the Harbour Master will communicate with the National Cyber Security Centre (NCSC). Any communications with other companies in the port will take place in consultation with the reporting party.

3. WHEN DOES THE REPORTING OBLIGATION APPLY?

The reporting obligation applies to companies required to comply with the Port Security Act (companies obliged to comply with ISPS). The reporting obligation also applies to Portbase and the nautical services providers[3]. All other companies are urged to submit a voluntary report. An immediate report of the IT disruption is mandatory when one the following conditions is met:

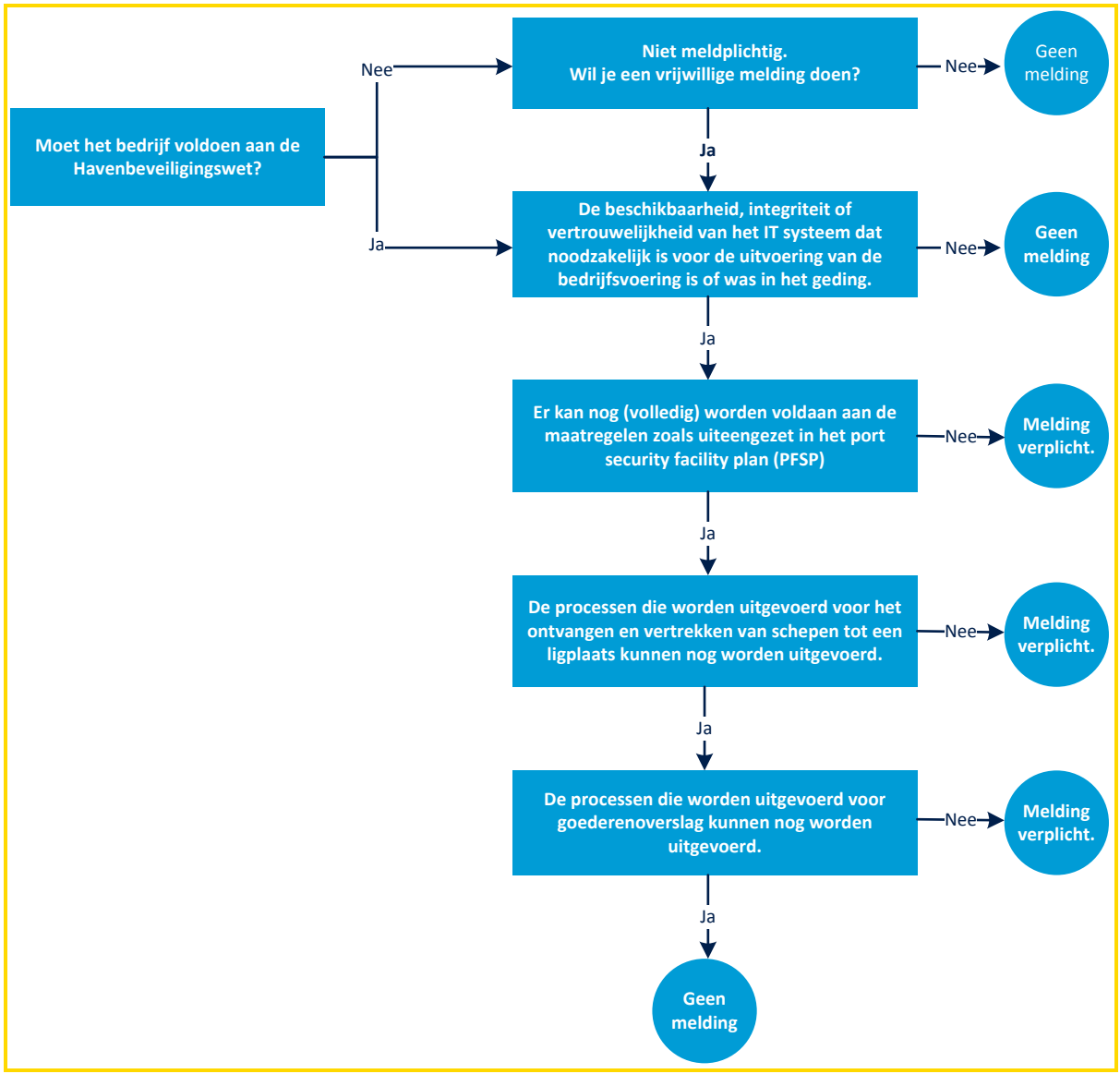
1) The company must comply with the Port Security Act or has a port security certificate, or the company is a nautical service provider.

2) The availability, integrity or confidentiality of the IT system necessary to implement the commercial operations was or is jeopardised.

3) The disruption will also bring about one (or more) of the three following consequences.
   a) It is no longer possible to carry out some of the port facility security plan measures.
      and/or
   b) Interruptions to processes for the receipt and departure of sea-going and other vessels, which are a potential threat to the company's security.
      and/or
   c) Interruptions to freight throughput processes, which are a potential threat to the company's security.

When none of the consequences as formulated under point three apply, the reporting of a disruption is not necessary. The overview below indicates when reporting is mandatory.

[3] Royal Boatmen's Association Eendracht (KRVE), the Dutch Maritime Pilot's Association and towing services.



When an intentional disruption (e.g. a cyber-attack) is involved that does not have consequences as formulated under point 3, it is still always desirable to submit a voluntary report. The Harbour Master can possibly use the information to offer a guide to other companies to protect their digital infrastructure from a cyber-attack. The report will enable the Harbour Master to assess whether the problem has wider impact and whether he should take measures to safeguard port area security and continuity.

4. HOW SHOULD A REPORT BE SUBMITTED?

Reports should be made to the Port Cyber Notification Desk by telephone on +31 (0)10 252 1005. The HCC Duty Officer will record the report and follow the verification protocol[4] (see appendix 1), in which at least the following information (as far as is known) should be provided:

- Details about the company concerned;
- Description of the disruption;
- Details of the anticipated security or other impact on commercial operations and any secondary effects;
- Information about the impact of the disruption on traffic handling and general security;
- Contact details of the staff member responsible for making the report and contact persons for the Harbour Master, Port of Rotterdam Authority Asset Management department and the Port of Rotterdam Authority Information Security Officer.

Reports should be made as quickly as possible to the Port Cyber Notification Desk. The initial report can be summarised: a brief report is preferable to an extensive report that is subject to delay, as a brief report can later be supplemented with the above information if necessary. The earlier a report is made, the greater the Harbour Master's chance of taking timely measures to reduce security and other consequences further on in the chain.

The Harbour Master advises companies that fall under the reporting obligation to record the reporting of IT disruptions in the standard (IT) incident process.

[4] The verification protocol is attached as appendix 1 to this policy document.

5. WHAT DOES THE PORT CYBER NOTIFICATION DESK DO WITH THE REPORT?

The reporting of IT disruptions enables the Harbour Master to estimate the potential impact on the port's logistics process. This is important, as a disruption can have far-reaching consequences for shipping and road traffic and other modalities. The report is therefore not only relevant to the reporting party but also to the other companies in the port.

The Harbour Master and the Port of Rotterdam Authority do not offer any IT support and do not focus on resolving the IT disruption. You can, however, expect the following action points from the Harbour Master and Port Authority:

- Determine whether additional measures are needed to support the secure handling of shipping traffic. This includes the deployment of additional patrols or the re-prioritisation of shipping.
- In consultation with partners, determine whether additional measures are needed to support the secure handling of road traffic and other logistics. This could include the establishment of a truck buffer plan and notifications to divert traffic.
- Determine whether the Port Crisis Team, chaired by the Harbour Master, should be convened. The Port Crisis Team will come into action if an IT disruption has consequences for multiple parties in the port and consultation is needed regarding logistical and nautical consequences and measures. The Port Crisis Team discusses the wider impact on the Port and all modalities. Depending on the composition of the Port Crisis Team, additional measures may be taken to support the security in the port and region.
- The company concerned may be invited to take part in the crisis team.
- Where necessary, the Harbour Master will inform third parties about the disruption and particularly the consequences of the incident. The Harbour Master can forward the report to the following partners:
    - Nautical service providers: to promote safety on the water.
    - The Seaport Police: to promote security in the port area.
    - The Rotterdam-Rijnmond Safety Region: to promote security in the port area and the region.
    - The National Cyber Security Centre: to satisfy the Harbour Master's statutory reporting obligation[5].
    - Other relevant stakeholders[6]: to promote digital defence in the port area.

The Harbour Master is aware that a report of an IT disruption can involve sensitive information. The sharing of information with the above bodies only takes place where this is necessary to safeguard port area security. Informing other (private) port facilities will always take place following agreement with the reporting party and will be anonymised, if required.

[5] Reporting obligation regarding the Data Processing Act and Cyber Security Reporting Obligation (WGMC). This act is expected to be replaced by the Network and Information Systems Security Act in 2018, in which the Harbour Master's reporting obligation is transferred.

[6] For example: Deltalinqs, DCMR Environmental Protection Agency Rijnmond, Rijkswaterstaat, Municipality of Rotterdam, etc.

6. WHAT DOES THE REPORTING PARTY DO?

The reporting party remains responsible at all times for resolving the IT disruption. The reporting party also remains responsible for its own digital infrastructure and for the security of its own site. In the context of these responsibilities, it is also possible that the company involved has a duty to report to other authorities, such as the Police or the Data Protection Authority.

The Harbour Master requests that the reporting party takes the following actions:

- Report the IT disruption and provide the requested information.
- If necessary: ask the Harbour Master to take measures to support the secure handling of shipping and road traffic, in which the reporting company gives an estimate of the expected impact on traffic control.
- Appoint a contact person (or contact persons) for the following topics:
    - Coordination of any water-based measures.
    - Coordination of any land-based measures.
    - Further technical and information security information.
- If necessary, participate in the Port Crisis Team at the invitation of the Harbour Master.
- Depending on the prognosis and the course of the IT disruption, provide the notification desk with interim updates.
- De-registering the disruption once operations have been resumed.

7. REPORTING OBLIGATION PRINCIPLES AND NOTIFICATION DESK

7.1 REPORTING OBLIGATION PRINCIPLES

Companies that must comply with ISPS, and Portbase and nautical service providers must report any IT disruption[7].

Companies that must comply with ISPS must report security incidents in accordance with EU Regulation 725/2004.[8] In the ports of Rotterdam and Drechtsteden, this procedure entails that companies should report physical or other security incidents to the Seaport Police.

With regard to the objective of the EU Regulation (improvements in ship and port facilities security against the danger of intentional unauthorised actions[9]), both physical and digital security fall under the concept of "security incident". After all, these cannot (certainly these days) be distinguished from each other. The 2004 EU Regulation already mentions the importance of computer systems and networks[10] and the IMO again focused attention on this in 2017 in the previously-mentioned resolution and guidelines.

The above entails that cyber incidents that are a threat to the port facility, shipping as well as the vessel/port interface, must be reported in accordance with that determined in the Regulation. What is new is that these incidents, unlike other security incidents, do not need to be reported to the Seaport Police, but to the Port Cyber Notification Desk.

Finally, the reporting obligation for Portbase applies on the basis of the Data Processing and Cyber Security Reporting Obligation Act (WGMC) and the upcoming Network and Information Systems Security Act. The companies that fall under the reporting obligation have a pivotal role in the Port of Rotterdam and are vital to the security and continuity of shipping and other traffic handling. In the context of the WGMC, individual agreements have or are being made with Portbase regarding the reporting of IT incidents. Individual agreements are also being made with nautical service providers.

[7] Royal Boatmen's Association Eendracht (KRVE), the Dutch Maritime Pilot's Association and towing services.

[8] Security incident: each suspected action or circumstance that is a threat to the security of a vessel, including the security of a drilling unit, a high-speed vessel, a port facility, a vessel/port interface or a ship-to-ship activity (art. 1.13 of requirement 1 of appendix 1 of the EU Regulation 725/2004.)

[9] art. 1 of EU Regulation 725/2004

[10] E.g. art. 15.3, 15.7 and 15.16 of section B of Appendix III of the Regulation

7.2 PRINCIPLES OF THE PORT CYBER NOTIFICATION DESK AT THE HCC

The decision to place the Port Cyber Notification Desk with the HCC of the Harbour Master's Division was agreed with the Seaport Police and the Rotterdam-Rijnmond Safety Region (VRR) and flows from the Harbour Master's statutory responsibilities. The Harbour Master is also in a position to take direct action to contribute to the security and continuity of the port logistics process. The following responsibilities lie at the basis of the notification desk at the HCC:

1. Port Security Act, Port Security Officer and the WGMC
   The Harbour Master was appointed as Port Security Officer to ensure compliance with the Port Security Act. Compliance with the Port Security Act is monitored through carrying out inspections. In the role as Port Security Officer, the Harbour Master is the authority for security in the port on behalf of the Mayor.

   The Mayor and the Harbour Master (mandated by the Mayor), are obliged under the Port Security Act to provide information for reporting IT or other disruptions that fall under the Port Security Act. By establishing the Port Cyber Notification Desk, the Harbour Master is creating a specific notification desk for IT disruptions. Based on the report, the Harbour Master can coordinate follow-up actions that contribute to the security of traffic in the port.

   In the context of the Data Processing and Cyber Security Reporting Obligation Act (WGMC), the Port of Rotterdam Authority and particularly the Harbour Master also have a reporting obligation to the National Cyber Security Centre (NCSC) when IT disruptions have a disruptive effect on society. It is also important that the Harbour Master has knowledge of the IT disruptions in the port area and is capable of making an estimation of any disruptive effect on society. The WGMC will be replaced by the Network and Information Systems Security Act in 2018, in which the reporting obligation is also incorporated.

2. Safe and organised shipping
   The Harbour Master is responsible for the safe, smooth, clean and secure handling of shipping in the Port of Rotterdam. In doing this, the Harbour Master has a responsibility to use expertise to support the secure and organised handling of traffic (particularly shipping traffic) wherever disruptions occur[11].

   Where IT disruptions have an impact on the reporting party's water-based operations, the Harbour Master will take action where necessary. This includes the deployment of additional patrols, the re-prioritisation of shipping and informing the nautical service providers.

[11] View the Harbour Master Rotterdam covenant via https://zoek.officielebekendmakingen.nl/stcrt-2004-2-p7-SC63196.html

3. Safe and organised road traffic
   The Port of Rotterdam Authority manages a large part of the port area infrastructure and works in close cooperation with Rijkswaterstaat to contribute to the security and continuity of road traffic.

   Where IT disruptions impact the reporter's land-based operations, the Harbour Master will forward the information to the Port Authority Asset Manager. This enables the Asset Manager to take action where necessary. This could include the establishment of a truck buffer plan to prevent congestion, and coordination with Rijkswaterstaat regarding the road signage.

4. Safe and organised operation of the other modalities (logistics)
   As well as the secure and orderly processing of shipping and road traffic, there is a rail and underground infrastructure in the Port of Rotterdam to be considered. These modalities also have interdependencies with other companies and information technology. IT disruptions can result in a temporary outage or congestion in these modalities, which could have consequences for port security. The Harbour Master can convene the Port Crisis Team to determine whether additional measures are needed to support the secure and orderly course of the other modalities.

8. ENFORCEMENT

The reporting obligation focuses primarily on anticipating the potential broader security effects of an IT disruption. Particularly by, in consultation with the reporter, warning other sections of the port as well as other companies, and offering a guide. In this way, submitting a report contributes to security and continuity in the port and to the commercial activities in the port area.

When a party that is obliged to report an IT disruption fails to do so, the Port Security Officer will contact the company concerned. The obligation to report will also be part of the annual evaluation in the context of the Port Security Act. Finally, the Harbour Master can impose a cease and desist order if a company continually fails to report an IT disruption.

9. IN CONCLUSION

The reporting obligation contributes to creating a culture in the Port of Rotterdam in which joint working on digital security is key. To foster such a culture, it is important that any reports are treated in confidence. The Port of Rotterdam Authority and the Harbour Master are extremely aware of the sensitivity of the information being shared and, together with public partners, will handle this with care.

Legislation and obligations regarding digital security are developing fast. New legislation and regulations focus mainly on safeguarding the security and continuity of IT and the privacy of data subjects. In this context, there is a lot of attention for the topic, also by the IMO, and more guidelines regarding cyber risk management will become available from various organisations. This development will also be manifest in the coming years in the requirements for the port facility security plan. Considering the developments, the Port Authority, the Harbour Master, Deltalinqs, the Municipality and the Police have made space for cooperation between all parties in the port: with cooperation and information sharing, security and continuity issues in the digital area should be addressed efficiently and effectively.

APPENDIX 1 - VERIFICATION PROTOCOL PORT CYBER NOTIFICATION DESK

1. Company:
    a. What is your name and position?
    b. What is the company name?
    c. What is the address?
    d. What type of company is it?[12]

2. Impact of the IT disruption on the reporting party's company:
    a. What consequences does the IT disruption have on your company?
    b. At what time did you first notice the IT disruption?
    c. Is the cause of the IT disruption known?
    d. What measures have you taken?
    e. When do you expect to have resolved the problem?

3. Port Security Act/ISPS:
    a. Does the company fall under the Port Security Act/ISPS?
        - If 'yes', continue to question 3b.
        - If 'no', move on to question 4.
    b. Do you still satisfy the port facility security plan requirements?
        - If 'yes', continue to question 4.
        - If 'no', continue to question 3c.
    c. What measures can you no longer carry out?

4. Security of traffic
    a. Does the IT disruption have consequences for land or water-based traffic handling?
    b. If yes, which problems do you expect with the traffic handling?[13]

5. The contact details of (this can be one and the same person):
    a. What are your contact details?
    b. Who can we talk with to discuss the handling of shipping traffic?
    c. Who can we talk with to discuss the handling of road traffic?
    d. Who can we talk with to discuss the handling of IT and IT security?

[12] Includes containers, dry bulk, liquid bulk, biobased, LNG, breakbulk, refinery, chemical industry, energy or offshore.

[13] The expected traffic impact is important to estimate whether measures need to be taken by the Port of Rotterdam Authority to guide the traffic on water and land in the right direction.

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

Port of Rotterdam