CYBER INCIDENT RESPONSE AND RECOVERY

Martijn Ebben | Cyber Security & Risk Officer VTS | Port of Rotterdam

IALA Cyber Security workshop | November 12-19, 2021

Port of Rotterdam

HOPE FOR THE BEST, PREPARE FOR THE WORST

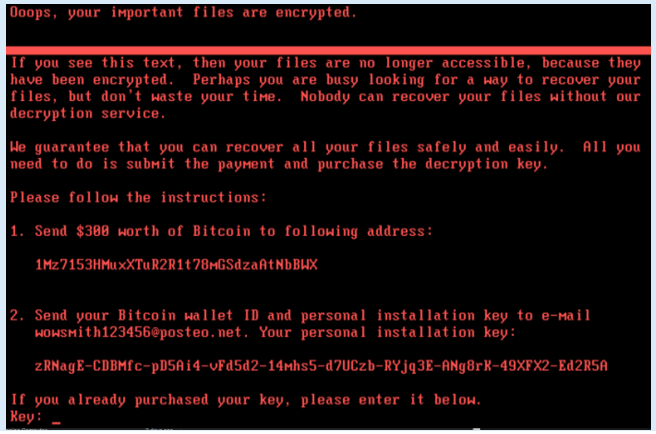
- Statistically, it is likely that every organisation will be confronted with a cyber incident at some point.
- Correct human behaviour and preventive technical measures will reduce the chance and scope/impact, but will never completely prevent incidents.
- A good preparation helps to recover more quickly after a cyber incident and maybe even “stay open” during the incident.

Port of Rotterdam

THE MAIN INGREDIENTS

1

PREPARATION



2

FIRST RESPONSE
or
"containment"

3

Crisis management

Coordinate and communicate

Business Continuity

Keep operating while the problem is solved

Recovery

Steps to return to business

Port of Rotterdam

PREPARATION

Once a hacker or malware attack is discovered, immediate response is required. No time to think. **Act**!

- Identify and document most important systems, networks etcetera. Identify and label relevant cables
- Know what (not) to do and what the acceptable impact may be;
  The risk of "losing" a laptop may not outweigh a disconnected VTS system
- Have your scripts in a red file folder somewhere you can quickly find it
- Have all necessary information on paper, including telephone numbers of management
- Have keys of doors that are usually opened by a computer-operated entry system
- Have pen and paper to make notes
- Use phones instead of computers – you may tip off the hacker that you detected him
- Have (validated) backups and installation media available
- Spare hardware might be good, especially in OT environments
- Make sure to always collect and save/protect system logs
- Sell the plan

Port of Rotterdam

FIRST RESPONSE

When a cyber incident is detected, the first response is up to the organisation itself. No time to call someone else.

- Determine impact and risk of spreading. Are compromised systems unavailable or unreliable?
- Determine appropriate action. This might be to not do anything at this point
- If invasive action is required, work with at least 3 people;
  - One communicates and makes sure the other two can focus on their tasks
  - One makes notes on the actions performed
  - One takes action (pull cables etc)
- It is usually better to disconnect systems rather than shut them down Key forensic artifacts will remain in volatile memory then
- Now, go and call your CERT or other expert for help and forensics

Port of Rotterdam

CRISIS MANAGEMENT

Not so different from any other crisis!

- A crisis management team may already be established within your company / organisation
- Adapt or amend to make it suitable for cyber incidents
- Instruct and/or educate applicable personnel

Can also be hired externally (CERT*)

*Cyber Emergency Response Team

BUSINESS CONTINUITY MANAGEMENT (BCM)

All about staying in business while (some) computer systems are unavailable or unreliable

- Is not required to be specific for cyber incidents. A good Business Continuity Plan can handle any disaster, even a COVID-19 pandemic
- Handles the effects of the cyber incident, not the incident itself
- Scenario-based. Scenarios may be quite similar to those for a power outage

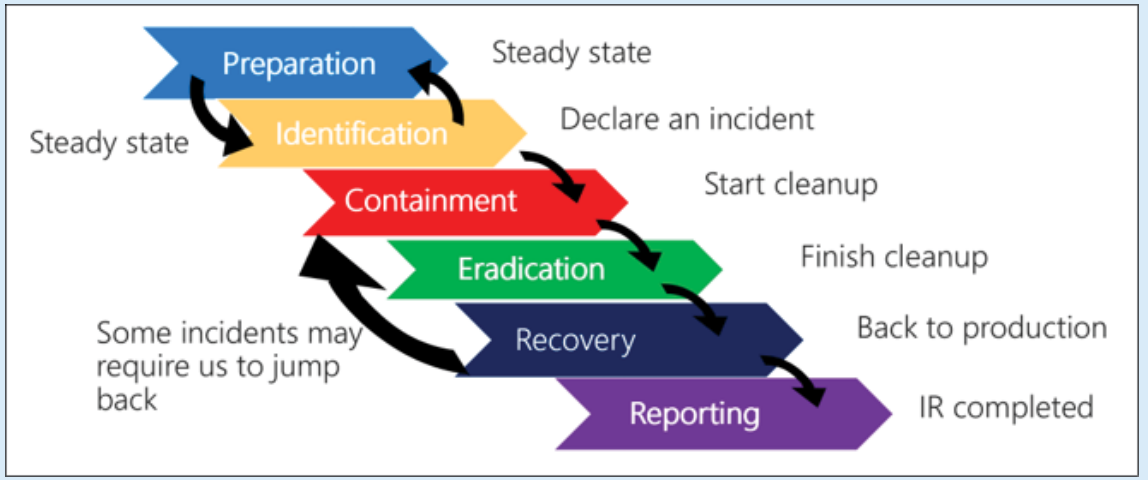
Should always be developed internally, but external assistance in the inital setup can be helpful

Port of Rotterdam

INCIDENT RECOVERY

Get back into business

- The technical part
- Clean or re-install all your systems
- Check
- Check again
- Check once more. Really sure?
- Turn them back on



Most organisations choose to hire this as a service (CERT). But internal knowledge is still key!

Port of Rotterdam

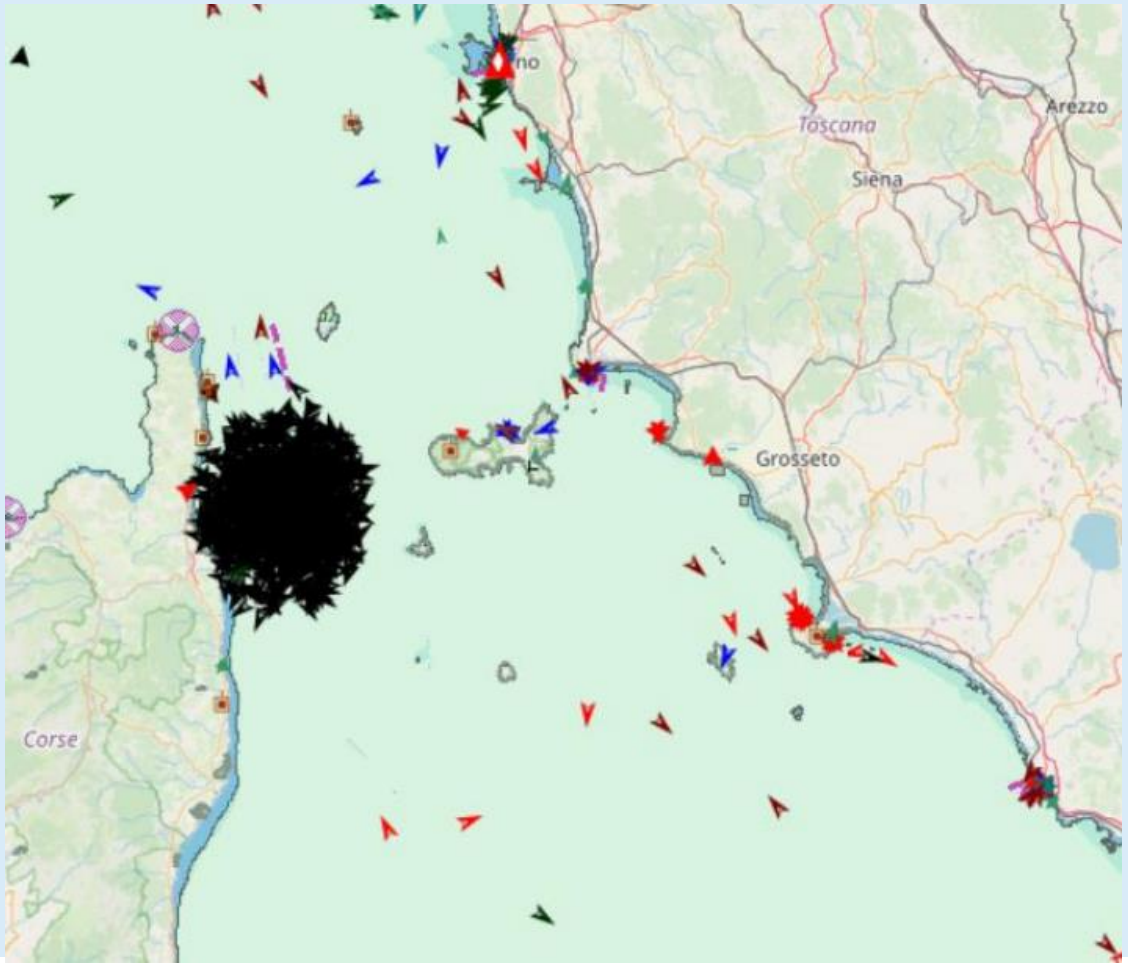
VTS, ATON AND MARITIME SERVICES IN THE CONTEXT OF E-NAVIGATION

How does this translate to the IALA domains?

- Can your VTS operate independently of other systems?
- What can happen to (virtual) AtoN?
- How will the unavailability or manipulation or Maritime Services (-data) affect operations and MASS?
- Determine policy: fail open or fail close?
  *What is the impact on confidentiality, integrity, availability and **safety** of this choice?*
- What alternatives do we have?
  handheld VHF transmitters, binoculars, lights, horns and other nautical signs

Port of Rotterdam

BCM: VULNERABLE MARITIME SERVICES



Most AtoN and Maritime Services operate in public area and are not very well protected.

Think of alternatives and if they are realistic

Service	Possible alterative
AIS	Radar CCTV Cameras
VHF	Telephone Audiovisual signs
GNSS	Visual positioning Time synchronisation via LTE

(examples)

Port of Rotterdam

JOIN WORKING GROUP 3 FOR A DEEP DIVE!

THANK YOU

Port of Rotterdam