IVR TECHNICAL LEAFLET

CYBERSECURITY IN INLAND NAVIGATION

SECURITY AGAINST CYBER ATTACKS

With the increasing technological developments in inland navigation it is essential to think about minimizing the risks concerning cyber attacks. A well thought out cybersecurity plan is a fundamental part of protecting your vessel and your company.

Therefore, IVR has put together this leaflet to give you some tips and tricks on how to implement a sustainable cybersecurity plan.

CYBERSECURITY

- IDENTIFY
- PROTECT
- DETECT
- RESPOND
- RECOVER

1 Identify

Which systems are vulnerable to attacks, which systems are vital to operations and who is responsible for them?

- Bridge

ECDIS systems may use online updating pay-as-you-sail chart folio access, but are they secure?

- Loading and stability programs

Copying or running authorised programs from third parties, such as loading programs, can introduce malicious software to the system.

- Engine room

Any device with an embedded computer can be attacked - don't leave any system vulnerable.

IS YOUR PASSWORD ONE OF THE MOST COMMONLY USED?

- 123456
- qwerty
- letmein
- admin
- dragon
- companyname123

Tip: a string of three random words makes a strong, easy to remember password.

2 Protect

Take these measures to prevent attacks from taking place.

- Regularly update devices to patch security issues.
- Password protect all devices and keep locked when not in use.
- Only allow designated crew to use high importance systems.
- Does the device have to be online and connected?
- Are firewalls installed throughout the network?
- Don't download software from suspicious sources.
- Don't open attachments on e-mails from unknown senders.
- Don't use external devices on the system without a security scan.
- If it looks or seems suspicious, STOP.

3 Detect

If an attack does happen, recognising it quickly can mitigate the damage.

- An up to date anti-virus program can monitor for any dangers.

- Scan computers, laptops and other external devices regularly.

- Did a download cause erratic behaviour? Be suspicious and isolate the system.

- Prepare a checklist to ensure no devices are missed.

4 Respond

Plan a clear means of getting back up and running as quickly as possible using a second system. Secondary devices and systems should be:

- Isolated from the main system.
- Kept up to date and ready to be used.
- Capable of running all critical operations.

USEFUL LINKS

- https://www.ccr-zkr.org/13020152-en.html
- https://twitter.com/Cybersec_EU
- https://www.pianc.org/publications/inland-navigation-commission/tg204
- https://europa.eu/european-union/about-eu/agencies/enisa_en
- https://www.shipownersclub.com/lossprevention/cyber-security

5 Recover

Get the primary system back running and analyse the cause.

RESET THE SYSTEM → RECOVER FROM BACK-UP → INVESTIGATE CAUSE → UPDATE PROCEDURES

Stay updated and secure

IVR is committed to making valuable contributions in the field of loss prevention.

Make sure you have a plan in place, following precautions and being ready to react could prevent your organisation from being the next victim of a cyber attack.