Cyber Threats and Cybersecurity - ENISA’s advice and support for waterborne transport

Dr. Athanasios Drougkas
Expert in Network and Information Security
ENISA – The EU Agency for Cybersecurity

Workshop on Cybersecurity in Inland Navigation
05 | 09 | 2019
POSITIONING ENISA’S ACTIVITIES

1. RECOMMENDATIONS ON CYBER SECURITY AND INDEPENDENT ADVICE

2. SUPPORT MS & EC IN POLICY IMPLEMENTATION AND HARMONISATION ACROSS EU

3. ‘HANDS-ON’ WORK, COLLABORATING WITH OPERATIONAL TEAMS THROUGHOUT EUROPE
THE MARITIME SECTOR IS UNDER ATTACK!

Hackers took ‘full control’ of container ship’s navigation systems for 10 hours – IHS Fairplay

Shipping firm warns that hackers may leak confidential information

Shipping company Maersk says June cyberattack could cost it up to $300 million

Police warning after drug traffickers' cyber-attack

The head of Europe’s crime fighting agency has warned of the growing risk of organised crime groups using cyber-attacks to allow them to traffic drugs.

The director of Europol, Rob Wainwright, says the internet is being used to facilitate the international drug trafficking business.

His comments follow a cyber-attack on the Belgian port of Antwerp.

Drug traffickers probed hackers to breach IT system that controlled the...
Backdoor Account Found in Popular Ship Satellite Communications System

Naval Dome exposes vessel vulnerabilities to cyber attack

More onboard cyber vulnerability has been revealed, with maritime cyber defence firm Naval Dome demonstrating yet more ways hackers can compromise ship safety.

Hackers can easily target container ships by hacking load plans due to its vulnerable messaging system

Security

Crappy IoT on the high seas: Holes punched in hull of maritime security

Researchers: We can nudge ships off course

Why 50,000 ships are so vulnerable to cyberattacks
MARITIME ASSETS – ATTACK SURFACE

Positioning systems
- Electronic Chart Display and Information System (ECDIS)
- Engine Control and monitoring systems
- Global Maritime Distress and Safety System (GMDSS)
- Automatic Identification System (AIS)
- Maritime ICS SCADA

Port service ships
- Special vehicles
- Physical floating barriers

Industrial Control Systems (ICS)
- ICS Communication Networks & Components

OT SYSTEMS & NETWORKS
- Port Community Systems
- Cargo Community Systems
- Fisheries Information Management Systems (FIMS)
- Proprietary Systems
- VTS/VIMIS
- Berth Management
- Port Corporate Systems
- Terminal Operations Management

Radio
- Protocols
- Servers
- Networks
- Switches
- Routers
- Cables
- LAN, VLAN
- Network security

Mandatory declarations
- Commercial and financial data
- Navigation data
- Control & Authorisation
- Operational data

Network & communication components
- Seaside connectivity
- Portuary infrastructure
- Buildings
- Energy
- Waste treatment systems
- Hinterland connectivity
- Safety & security

OT END-DEVICES
- Port facility specific lay-out
- Vessels berthing
- Vessels loading and unloading
- Temporary Storage
- Hinterland connectivity

IT SYSTEMS
- Workstations,
- Walls of screens etc.
- Mobile devices

Detection systems
- Emergency communication systems
- Access control systems
- Traffic monitoring systems
- Surveillance & inspection systems
- Evacuation systems
- Identification systems
- Alerting systems

Safety & security systems
- Port authority staff
- Permanent commercial staff
- IT/OT staff
- External staff
- Ship crews
- Passengers
- General public

People

INFORMATION & DATA

IT END-DEVICES

FIXED INFRASTRUCTURE

ASSET TAXONOMY
MARITIME CYBER THREAT LANDSCAPE

THREAT TAXONOMY

NEFARIOUS ACTIVITY & ABUSE
- Denial of Service
  - Malware
  - Brute force
  - Identity theft
- Phishing / Social engineering
- Targeted attacks
- Abuse and theft of data
- Manipulation of information

PHYSICAL ATTACKS
- Fraud
  - Sabotage
  - Vandalism
  - Theft
- Unauthorised access
- Terrorism
- Hacktivism
- Coercion, extortion or corruption
- Piracy / Organised crime

OUTAGES
- Systems
  - Devices
  - Navigation and communications systems
  - Main supply systems
- Failure or disruption of Service providers

FAILURES AND MALFUNCTIONS
- Environmental disasters
  - Natural disasters

UNINTENTIONAL DAMAGE
- Main supply outage
  - Network outage
  - Absence of personal
  - Loss of support

EAVESDROPPING INTERCEPTION HIJACKING
- Use of unreliable source
  - Erroneous administration of IT/OT systems
  - Resulting from penetration testing
  - Data deletion
  - Third party security failure
  - Information leakage

INTERCEPTION OF EMISSIONS
- Interception of sensitive information
- Man in the middle / session hijacking
- Network Reconnaissance
- Network traffic manipulation
CYBER SECURITY IN THE MARITIME SECTOR – SITUATIONAL ANALYSIS

- Cybersecurity gaining more attention but still relatively low awareness and focus on maritime cyber security
- Emerging standards/guidelines from IMO, industry etc.
- Complexity of the maritime ICT environment including SCADA and emerging IoT usage
- Fragmented maritime governance context
- No holistic approach to maritime cyber risks and diversity between different actors in maritime
- Overall lack of direct economic incentives to implement good cyber security in maritime sector
OTHER MARITIME REGULATIONS, GUIDELINES AND STANDARDS

- Guidelines on maritime cyber risk management (IMO)
- Maritime cyber risk management in safety management systems (IMO)
- The Tanker Management and Self Assessment - TMSA (OCIMF)
- The Guidelines on Cyber Security Onboard Ships (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI)
- The European Union Maritime Security Strategy (EUMSS)
- Cyber Security Awareness (AMMITEC)
- Recommendations on cyber safety for ships (IACS)
RELEVANT ENISA REPORTS

- 2011: Analysis of Cyber Security Aspects in the Maritime Sector
- 2016: Securing Smart Airports
- 2016: Cyber Security for Smart Cities
- 2016: Cyber Security and Resilience of Intelligent Public Transport
- 2017: Cyber Security and Resilience of smart cars
- 2017: Communication network dependencies for ICS/SCADA Systems
ENISA’S ON-GOING WORK IN MARITIME

2019 Study: Port Cybersecurity
- Port CISOs/CIOs
- Good practices / Recommendations
- Validation workshop – November 26th

NIS Directive Transposition
- National Approaches
- OES identification, Security Measures, Incident Reporting

Other Activities
- Collaboration with DG MOVE and EMSA
- Stakeholder Engagement (MARSEC, SAGMAS, Associations, Industry etc.)
- Raise awareness via workshops and meetings
PORT CYBERSECURITY WORKSHOP

ENISA MARITIME CYBERSECURITY WORKSHOP

STRENGTHENING THE CYBERSECURITY OF EU PORTS

26 November 2019

https://www.enisa.europa.eu/events/enisa-maritime-cybersecurity-workshop
TRANSSEC – MARITIME WORK STREAM
BUILDING CYBERSECURITY SKILLS

Cyber Exercises

Cybersecurity Training

Cyber Security Education

NIS School
OTHER ENISA REPORTS / ACTIVITIES

• ISACs good practices
• Support for existing sectorial ISACs

• Annual report with horizontal and sectorial threats
• Available as online tool

• Risk Management for SMEs
• Business Continuity for SMEs
• Self Assessed Risk Management (SARM)
THE NETWORK AND INFORMATION SECURITY DIRECTIVE
THE EU CYBERSECURITY CERTIFICATION FRAMEWORK

1: Identification of strategic priorities
2: Preparation of a Candidate Scheme
3: Adoption through an Implementing Act
4: Certification against this scheme and issue of an EU Cybersecurity Certificate
THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu