FEPORT

The Federation of European Private Port Companies and Terminals

# Position Paper on cyber security challenges in ports

FEPORT represents 1225 private seaport companies and operators which perform cargo handling activities and a wide range of other operations in European ports. FEPORT members employ more than 390.000 port workers paying taxes in the EU and supporting its growth.

Private port companies and terminals are modernizing EU ports by innovating processes, investing (56 billion Euros over the last ten years) in green equipment, digitalization, prevention of cyber risks, artificial intelligence, reskilling and upskilling of port workers.

Private port companies and the maritime logistics sector at large are facing the challenges of the fourth industrial revolution. Digitalization of the sector and the use of automation entail more investment in the prevention of cyber risks that would threaten business continuity.

**What are the biggest challenges in terms of cyber security for port companies in these days?**

Ports and private port companies as many other sectors rely increasingly on technologies to be more competitive, comply with some standards and policies and optimize operations. This brings new stakes and challenges in the area of cybersecurity, both in the Information Technologies (IT) as well as in Operation Technologies (OT) worlds.

Due to the number and diversity of stakeholders taking part in port operations and with whom port companies interact, the challenge is to overcome the technical complexity of port IT and OT systems of the different port stakeholders who use different systems that are developed, managed and maintained by different teams or entities. Another challenge lies in the fact that OT systems, more vulnerable than IT systems, are protected because they are separated from IT systems and networks. But, increasingly, IT and OT systems and networks, become more and more dependent and interconnected thus the importance given by port companies to the resulting risks.

There is however a need to find a right balance between business efficiency and cybersecurity, especially by guaranteeing the continuity of services while keeping IT and OT secure.

The European Union has identified ports as critical infrastructure and defined the ports as “any specified area of land and water, with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations” in article 3(1) of Directive 2005/65/EC.

Ports play a crucial role at different levels for many sectors and have been the successful pioneers in Europe for interconnecting the different types of transport. As a main vehicle for European imports and exports (food, commodities, etc.) with the rest of the world, ports enable also trade and contacts between all European nations.

For a number of years, ports have been undergoing a digital transformation in order to meet emerging challenges and port companies have been playing a major role in this respect. They are optimizing existing processes and introducing new capabilities, such as automation and real-time monitoring of operations. This digitalization has been centered around the interconnectivity of Information Technology (IT) and Operation Technology (OT) assets and the introduction of new technological enablers, such as big data and Internet of Things (IoT).

The complexity of the port ecosystem due to the number and diversity of stakeholders taking part in port operations is an important challenge because the level of awareness with respect to cybersecurity might not be the same for all actors in a port. However when it comes to port companies and terminals as there have been huge investments in IT and OT, time and budget, awareness and training regarding cybersecurity as well as the recruitment of qualified people to deal with cybersecurity has also become a top priority.

**What are the typical types of cyber security incidents in the port industry?**

The shutdown of the port operations is a much-feared impact by the port ecosystem as it can harm strongly the commercial operations, the security of supplies of essential goods for the country and also pose issues with respect to safety, security and fluidity of the cargo flows.

Port ecosystems may hold critical information, whether it is personal information (crew or passenger data), critical commercial information or National security information about supply chains or other information about container lists of cargo.  A port can lose a lot of money due to the stop of operations or for repair budget, in case of damage on its systems and infrastructure.

Industry is learning from incidents such as the NotPetya Ransomware incident and its impact on Maersk and the wave of ransomware attacks in the port of San Diego.

Cybersecurity challenges are associated with the supply chain. Cooperation between different actors of the supply and logistics chain is therefore needed and will certainly intensify in the coming years. It is a sensitive topic.

In ports, many companies are involved in port operations (port operators, Port Authorities, pilotage companies, shipping companies, etc.). It is crucial to ensure that all are involved in cybersecurity matters and aware about how they contribute to the port operation security.

The maritime sector is historically very aware of safety and security matters, but cybersecurity is not fully integrated by all stakeholders be it on the seaside or shore side. The enforcement of technical cybersecurity basics, like network segregation, updates management, password hardening, segregation of rights, etc. is broadly implemented.

## Expectations from policy makers

The NIS Directive is a first base to implement cybersecurity measures and concerns some of the stakeholders in the maritime sector. Port companies are involved in the work currently done by ENISA (European Union Agency for Cyber security) at EU level and are looking forward to continuing the constructive dialogue.

IT and OT systems are deployed by port companies who decide about the technical requirements needed to ensure good and secure operations. It is important that any assistance or initiative from EU policy makers remains a bottom up approach.