How can EU ports tackle new cyber threats?

ENISA, the European Union Agency for Cybersecurity publishes "Good practices for Cybersecurity in the Maritime Sector - Port Security", a report providing guidance for ports to strengthen their cybersecurity.

Published on November 26, 2019



Tagged with

* [Cybersecurity](https://www.enisa.europa.eu/search?Subject%3Alist=Cybersecurity)
* [ENISA](https://www.enisa.europa.eu/search?Subject%3Alist=ENISA)
* [Port](https://www.enisa.europa.eu/search?Subject%3Alist=Port)
* [Maritime](https://www.enisa.europa.eu/search?Subject%3Alist=Maritime)

**State of Play of Port Security**

Port stakeholders are facing more and more cybersecurity challenges with the emergence of new threats, regulations and increased digitalisation. Major incidents such as ransomware attacks targeting ports had a considerable impact on the economy.  As such, ports must address cybersecurity as a top priority in order to ensure their safety, security, compliance and commercial competitiveness, while unlocking the full capabilities of their digital transformation.

In light of increasing digital transformation of port ecosystems, the [ENISA Port Cybersecurity - Good practices for cybersecurity in the maritime sector report](https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/) highlights good practices to address new cybersecurity threats. Specifically, the emergence of the ‘SmartPorts’ concept brings new challenges for the deployment of emerging technologies (IoT, blockchain, big data, cloud, automation, AI etc.) which often leads to greater exposure of port systems. While ports have traditionally been concerned with physical security and safety, they must now integrate cybersecurity in their global strategy.

ENISA’s Executive Director, Juhan Lepassaar, stated: “*Given the economic importance of ports in EU trade, the protection of essential port operations against cyber-attacks becomes paramount. It is important to equip EU ports with all necessary tools and knowledge to address cybersecurity concerns as they undergo their digital transformation. The report aims to provide port authorities and terminal operators, especially those in most need of relevant guidance, with a comprehensive set of good practices.”*

**Key Findings**

The report lists an extensive set of security measures that port authorities and terminal operators can adopt to develop a security baseline. The main measures identified are described below and intend to serve as good practices for people responsible for cybersecurity implementation in Port Authorities and Terminal Operators:

* Define a **clear governance** around cybersecurity at port level, involving all stakeholders involved in port operations.
* Enforce the **technical cybersecurity basics**, like network segregation, updates management, password hardening, segregation of rights, etc.
* Consider **security by design** in applications, especially as ports use many systems, some of which are opened to third parties for data exchange.
* Enforce **detection and response**capabilities at port level to react as fast as possible to any cyberattack before it impacts port operation, safety or security.

**What does the study hope to achieve for its target audience?**

Developed in collaboration with several EU ports, this report intends to provide a useful foundation on which CIOs and CISOs of entities involved in the port ecosystem, especially port authorities and terminal operators, can build their cybersecurity strategy. Furthermore, the study can also be useful for other stakeholders in the broader community within the port ecosystem, such shipping companies and maritime policy makers.

In particular, this report intends to:

* Identify the main port infrastructure and services (maritime cargo, passenger and vehicle transport, fishing activities), as well as establish an overview of stakeholders involved in port ecosystems and define a comprehensive asset taxonomy;
* Establish a high-level reference model describing port systems and the data flows between them and other external systems;
* List the main cybersecurity challenges that port stakeholders are facing today and are likely to face in the future and define a complete threat taxonomy that lists the different threats and their possible impacts;
* Describe cyber-attack scenarios that the port ecosystem could face, influenced from cyber-attacks that have already occurred in the maritime sector; and
* Provide a list of cybersecurity measures that highlight best practices and help improve the cybersecurity maturity of port ecosystems.

**Next steps**

Still, people responsible for port cybersecurity are encouraged to go beyond the good practices proposed in the ENISA report and address additional topics as well, such as **awareness raising** about cybersecurity at board and staff level, **information sharing** amongst port operators, addressing **cybersecurity in the supply chain** and integrating **interdependencies cybersecurity risks** in the overall cyber risk management process.

ENISA intends to keep playing its role in the continuous process of strengthening the cybersecurity of the EU maritime sector by addressing key issues and recommendations in the following years, supporting policy and regulatory developments and facilitating information sharing and the exchange of good practices between maritime stakeholders.