ABOUT

- Project start in September 2015
- Thirteen partners from research, software development, logistics and ports
- Partners‘ countries: Austria, England, Germany, Greece, Italy, Romania and Spain
- Duration 30 months
- Budget 3.55 m€, funded within the EU Horizon 2020 programme with 3.1 m€

This project has received funding
from The European Union´s Horizon 2020
research and innovation programme
under grant agreement No 653212.

BACKGROUND

THE MARITIME SUPPLY CHAIN IS AT RISK!

Not only do piracy attacks and global terrorism threaten the transport of goods and passengers, also cyber criminal activity focuses on information infrastructure. Ports are global maritime transport nodes where high volumes of goods are handled and crucial data and information are exchanged. The hardware and software assets, comprising the port‘s critical information infrastructure (CII), are more vulnerable to cyber attacks than the information infrastructure of a single link along the supply chain. This high vulnerability is associated to the great number of different actors who access the information related to these CII.

International, European and national guidelines and standards for the protection of CII exist and could be applied to ports, to bolster their security and resilience capabilities. It is expected that these standards will be declared as mandatory for sea ports in the near future, hence they are already considered in the course of MITIGATE.

OBJECTIVES

The project goal is to develop the standards-based MITIGATE system for collaborative managing, forecasting and visualizing risks in maritime supply chain’s CII. This is enabled through a software framework that shall seamlessly expose security gaps.

Participating ports have to conduct an in-depth analysis and evaluation of their CII. Having established the actual status of the CII, a new risk assessment can be initiated, enabling the port to detect digital and hardware vulnerabilities and potentially alleviate their security risks. The maritime supply chain and the respective information flow do not start or end in ports. In order to protect the port supply chain from security threats that may cause cascading effects among the actors, their collaboration is of vital importance.

MITIGATE builds on the cooperation of participating ports, disclosing new and relevant cyber threats. The larger the group of ports and supply chain partners that uses the MITIGATE system, the more accurate the risk assessment in the supply chain and the better the partners can protect their CII.

PARTNERS

Fraunhofer CML

GRUPPO Maggioli

UNIVERSITY OF PIRAEUS RESEARCH CENTER

FEPORTS
Instituto Portuario de Estudios y Cooperación de la Comunitat Valenciana

SingularLogic
Innovation at your doorstep

IMSSEA
IMO

University of Brighton

OAΠ
PIRAEUS PORT AUTHORITY S.A.

AIT
AUSTRIAN INSTITUTE OF TECHNOLOGY

PORT OF RAVENNA AUTHORITY

dbh
dbh Logistics IT AG

FUNDACIÓN valenciaport

Autorità portuale Livorno

Hansestadt Bremisches Hafenamt


© xy - Fotolia.com


© Zacarias da Mata - Fotolia.com

CONTACT US

PROJECT COORDINATOR

Fraunhofer Center for Maritime Logistics
and Services CML
Dipl.-Logist. Reiner Buhl

TECHNICAL MANAGEMENT

University of Piraeus
Associate Professor Nineta Polemi

LinkedIn

INFO@MITIGATEPROJECT.EU
WWW.MITIGATEPROJECT.EU

PROTECTING PORTS' IT INFRASTRUCTURE

MITIGATE

Multidimensional, integrated, risk assessment framework and dynamic, collaborative Risk Management tools for critical information infrastructure