MITIGATE

NEWSLETTER 01

September 2016

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

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

INTRODUCTION

Our modern information society is depending on functioning and reliable information and communication structures. This fact is used by criminal offenders more and more frequently. Damages caused by cyber attacks have been increasing for years. As the supply chain is also a risk chain, companies are increasingly affected by incidents regarding the information safety of their customers, partners or suppliers and therefore have to face new, cyber specific challenges.

Based on the growing international linking of companies and especially terminals as nodes in global freight transport, the topic of IT security is gaining in importance. Although IT safety plays an important role for the international supply chain, the modern methods of risk management have not paid a lot of attention to it so far.

Therefore from September 2015 on, eleven partners from research and development, logistics and port administrations from Germany, Austria, Italy, Spain, United Kingdom, Greece and Romania, are going to develop the innovative Risk Management System MITIGATE, which is intended to close this gap. The core of MITIGATE Risk Management System is an open environment that can be used to simulate and analyze possible risk scenarios.

Furthermore, these simulations can help to better predict and therefore avoid hazards in the future. Moreover the system can provide for more transparency in handling risks and hazards.

© Marco2811 - Fotolia.com

Container Terminals in twilight - cyber criminals do not need the darkness

MITIGATE USER ADVISORY BOARD STATEMENT

Port authorities, terminal operators, logistics IT providers, forwarders and shipping companies are facing a constant risk of being successfully attacked by cyber criminals. Because of the close connections between companies in supply chains, attackers could work their way from one company IT system into another.

Therefore, efforts have to be made to better secure maritime supply chains, their operators as well as customers IT systems, their cargo and their data.

MITIGATE aims to be a solution to increase the security level. It will help the IT security personnel to better identify potential vulnerabilities and also to mitigate the risks.

We expect that MITIGATE will enable all actors of one supply chain to analyze and mitigate risk together and significantly increase IT security.

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

SUPPORT FROM MARITIME SUPPLY CHAIN COMPANIES AS PILOT USERS

MITIGATE aims at securing critical information infrastructures along the maritime supply chain. Thereby the objectives of the MITIGATE system follow national and international regulations and legislation. MITIGATE is expected to fulfill the security demands required by maritime stakeholders.

To ensure reliable use of the MITIGATE system in the working environment, pilot users take part in the project. Right from the beginning the Ports of Bremen in Germany, Piraeus in Greece and Livorno in Italy are engaged in the project consortium. Later on, after a thorough internal test phase, more pilot users will join the project.

For each single pilot site, the project partners will review roles, responsibilities, organization structures, assets, security processes, logistics processes and more; ensuring confidentiality through a strict declaration. For each pilot site, the system will be localized and adapted to organizational structures and stakeholder's roles.

A pilot testing period (of approximately two months) is foreseen. In the scope of this testing period, end-users will have the opportunity to use the MITIGATE system and tools, with a view to identifying issues or problems early on that could adversely impact the pilot operations. Still there is a possibility to participate: Port security officers and IT personnel of port facility operators, logistics and shipping companies, port authorities and supply chain participants have the chance to try the software in advance. If you are interested in the MITIGATE project or in participating during the test phase of the software, please do not hesitate to contact the project consortium: info@mitigateproject.eu

NEW DEVELOPMENTS IN MARITIME CYBER REGULATION AND GUIDELINES

Until recently, guidelines, standards or regulations on cyber security for ports and the maritime supply chain did not exist. The International Maritime Organization (IMO) International Ship and Port Facility Security (ISPS) Code mainly deals with physical security of ports and vessels; only mentioning that communication has to be possible in case of an incident. But there are proposals in order to extend the scope of the ISPS Code and to include cyber security. In June 2016, IMO has published "Interim Guidelines on Maritime Cyber Risk Management" and further organizations have been working on this topic.

The Baltic and International Maritime Council (BIMCO) published "The Guidelines on Cyber Security Onboard Ships" in January 2016 and the United stated Coast Guard a document on "Cyber Risks in the Marine Transportation System". Also Lloyds Register is visibly active: In February 2016, a "Guidance Note" on "Cyber-enabled ships" about cyber risks for state of the art computer supported ship operation has being issued. In July 2016 another "guidance document" on "Cyber-enabled ships" with a focus on autonomous ships was made public.

These documents state that important measures of higher security levels for computers and data are i.a. better software, improved processes and trained staff.

Also European Union institutions are working on the computer crime topic. A "Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union" is currently under discussion within the Council and its preparatory bodies.

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

THE NEED OF RISK ASSESSMENT, USER REQUIREMENTS AND THE MITIGATE APPROACH

The increasing digitization of more and more business processes leads to access and exchange opportunities for digital information along the maritime transport chain.

It is recognized that in the maritime sector risk management has been traditionally more focused on physical security (e.g. IMO ISPS, EC725/2004 regulation), thus a gap is identified between sector specific risk management approaches and the need to protect an increasingly more important maritime cyber infrastructure. According to surveys[1], cyber risks rank among the most important risks for business interruption and supply chain disruption of companies and are expected to become the most important risk in the future.

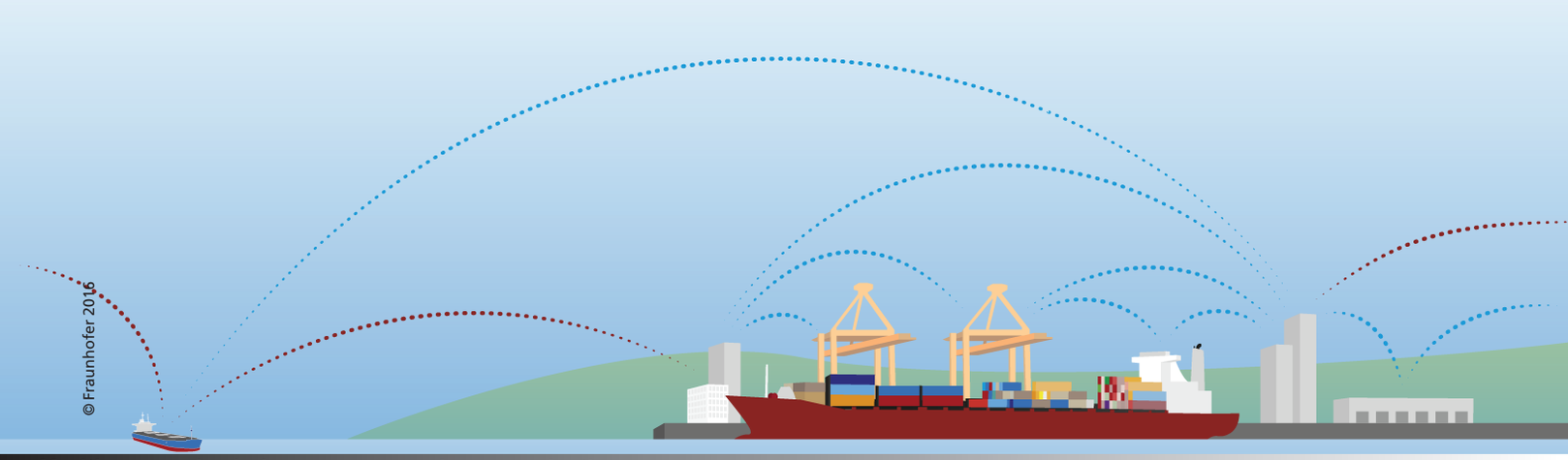
In the MITIGATE project, the partners examine the data security of maritime supply chains, e.g. of liquefied natural gas, container and bulk goods, as well as vehicle transport chains.

A first (nonrepresentative) survey has revealed that nearly two thirds of the respondents do not carry out a risk assessment of their IT infrastructures so far. From the perspective of the respondents, the most important cyber assets are corporate networks (between 50 and 60%) as well as databases and operational applications (65 to 75% respectively). In addition, conformance to national and international regulations and standards was confirmed as a top requirement.

To build a thorough basis for the MITIGATE system, relevant security management standards were identified in the first months of the project duration, and the requirements associated with the MITIGATE framework are now being validated. To analyze and develop security requirements, attention had to be paid on how these capture and refine security goals. Processes and methodologies to model such requirements, goals, problems or threats are numerous; e.g. KAOS, Secure Tropos, UMLsec and Trust Modelling. For MITIGATE purposes, the project partners decided to use Secure Tropos. This tool proved mightiness and suitability in earlier projects concerning risk analyses in the maritime supply chain.

But the analysis of an IT system, its cyber assets and software applications, is not enough, considering the complex cross-linked digital relations among the elements a transport chain consists of. It is not realistic to expect a thorough defense from all possible cyber attacks. Thus, and in order to provide a concrete background for the MITIGATE toolset, a review of the state of the art in mathematical approaches to supply chain risk assessment was also conducted. Tools such as queuing theory, game theory, simulations, fuzzy and nonlinear programming have already been employed to solve problems in supply chain systems, transportation systems and logistic systems, but as they were not conceived to address specifically cyber security issues in the supply chain novel approaches need to be explored by the project. The chosen approach involves the use of Big Data analysis to exploit diverse sources of information on threats; such as logs, social media and crowd sourcing.

1 Allianz SE & Allianz Global Corporate & Specialty SE (2015) „Allianz Risk Barometer 2015“
Allianz SE & Allianz Global Corporate & Specialty SE (2016) „Allianz Risk Barometer 2016“



Maritime supply chain resources and communication

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

PARTNERS

Fraunhofer CML

University of Piraeus Research Center

SingularLogic – Innovation at your doorstep

University of Brighton

AIT Austrian Institute of Technology

dbh Logistics IT AG

Autorità portuale Livorno

Gruppo Maggioli

FEPORTS – Instituto Portuario de Estudios y Cooperación de la Comunitat Valenciana

IMSSEA – IMO

OAΠ Piraeus Port Authority S.A.

Port of Ravenna Authority

Fundación Valenciaport

Hansestadt Bremisches Hafenamt

KEY FIGURES

- Thirteen partners from research, software development, logistics and ports
- Partners‘ countries: Austria, United Kingdom, Germany, Greece, Italy, Romania and Spain
- Project duration: from September 2015 till February 2018
- Budget 3.5 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.

DATES / MEET MITIGATE

SMM, September 6.-9. 2016, Hamburg

NMIOTC Cyber Security in the Maritime Domain, October 4.-5. 2016, Chania/ Crete

11th Int. Conference on Critical Information Infrastructure Security, October 10.-12. 2016, Paris

PROJECT COORDINATION

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

TECHNICAL MANAGEMENT

University of Piraeus
Associate Professor Nineta Polemi

CONTACT

info@mitigateproject.eu

MITIGATE

www.mitigateproject.eu

LinkedIn

www.linkedin.com/grps/MITIGATE-8472607

twitter.com/MITIGATE_EU