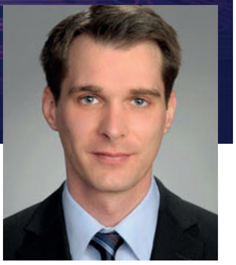

DETECT AND CONTROL CYBER RISKS

IN THE MARITIME SUPPLY CHAIN

Claudia Bosse, Scientific Researcher, and Martin Stamer, Scientific Researcher,
Fraunhofer CML, Hamburg, Germany

The IT infrastructure of ports, comprising hard- and software assets of the companies engaged in transport and goods handling in the maritime supply chain, is particularly vulnerable in the present day. Ports are located at the interface of information flows from many different users and countries that access and exchange capabilities for digital information. Every data interface means a potential threat in form of a possible entry point for unplanned access to the systems behind. The ongoing digitalization will result in even more complex and a higher degree of networked IT-systems and so will the number of electronic interfaces to business partner systems in supply chains increase, which cannot be supervised and controlled by the single company.

In order to ensure that these processes and interconnections don‘t allow malware to shut down operations or allow manipulation of data for illegal purposes, a solution to identify threats along the supply chain is urgently needed. Although not many cyber incidents concerning the maritime supply chain are reported, due to the fears of the involved companies with regard to damage to their reputations (or maybe even worse due to a lack of knowledge and awareness), the following incidents show the bandwidth of possibilities:

- Containers containing drugs were misled without early recognition
- Customs systems were shut down, stopping operations for hours, probably to press ransom
- The disruption of the GPS-signal stopped operations of vessels as well as of terminal cranes that store and locate containers basing on GPS for the same reason
- Piracy attacks use AIS-signals to identify vessels and hack into the shipping companies systems to identify their loaded goods
- May 12, 2017: Global ransom ware campaign known as “WannaCry” was detected, affecting various organizations with tens of thousands of infections in over 150 countries

CYBERSECURITY IN CHANGING LANDSCAPE

The Verizon Data Breach Report 2017 illustrates that the transportation sector still lies not in the focus of cyber attackers. Of the more than 42,000 incidents of data breach reported only 63 took place in the transportation sector. Nevertheless, experts assume that the growing connections of digital assets due to the development of the internet of things and maritime 4.0 solutions will enable more, easier and more effective cyber-attacks.

A global study among risk managers and risk experts rated cyber incidents as the third highest business risk worldwide for all sectors and are expected to become the highest business risk in the future. In Europe cyber risks are rated as the second highest and in Germany as the highest business risk.

Now how do attackers find the way into digital assets despite existing security shields? Three quarts of breaches were perpetrated by outsiders, regarding the Verizon Report. Thereof, more than 60% were featured by hacking into the system, meaning more than 80% of the incidents use of stolen or weak passwords. Another common way to avoid the installed security systems is the installation of malware via emails.

These breaches are tackled by security guidelines, e.g. from the Baltic and International Maritime Council (BIMCO). They provide effective advice and awareness-rising posters for the use on board show the need, but also the chances to avoid the biggest part of incidents by giving striking rules for the use of passwords and private communication devices.

REGULATIVE MEASURES

Firstly, the International Ship and Port Facility Security Code (ISPS) was launched by the IMO in 2002. The ISPS Code consists of a comprehensive set of measures to enhance the security of ships and port facilities. ISPS deals with the issue of IT security only on a rough overview level and does not provide distinct methods, tools or roles. However, it is stated that for ship security and port facility security, IT as such should be used in order to identify and take preventive measures against security incidents.

The Information Security Management System (ISMS) is a standard that specifies requirements for the establishment, implementation, monitoring and continuous improvement of information security in organizations. To do so, the ISMS provides an overall management and control framework for an information security risks and is defined in ISO/ IEC 27001.

ICT systems of ports are classified 'Critical Information Infrastructures', because ports are very important for the unrestricted supply, trade and economy of a country. In July, 2016 the EU adopted the Network and Information System (NIS)-Directive. The directive aims to reach a common level of security of NIS in the EU. This process shall be supported by the European Union Agency for Network and Information Security (ENISA) and protected by Computer Security Incident Response Teams (CSIRT).

Further, the IMO issued interim guidelines on maritime cyber risk management in 2016 and the US promotes Information Sharing and Analysis Organizations ISAO, e.g. the Maritime & Port Security Information Sharing and Analysis Organization. Not least, the International Association of Classification Societies (IACS) in shipping reacts to cyber threats with a cyber-systems panel that was installed in 2016. The focus of this panel lies on the early development of cyber resilient onboard systems.

Still, the above description of regulation and guidelines cannot be exhaustive as there are more national initiatives and specific guidelines than can be illustrated here.

MITIGATE

Obviously, stakeholders in the maritime supply chain are aware of threats, and the framework to act is set. This is why a consortium of companies from the software industry, academia and port authorities joined together to find a solution.

The project partners of MITIGATE (Fraunhofer, University of Piraeus Research Center, Austrian Institute of Technology, Maggioli, SingularLogic, Valencia Port Foundation, Ports of Piraeus, Ravenna, Livorno and Bremen, dbh Logistics IT, and the University of Brighton: The project receives funding from the European Commission) have developed a dynamic software solution which allows ports, logistics or administration companies to check the software, hardware and gateways they use for vulnerabilities of cyber-attacks.

If a new vulnerability gets detected and disclosed to the public, normally appropriate counter measures are following soon, but a large amount of users seem not to realize the publication of the vulnerability as well as of the counter measures. For example, the aforementioned WannaCry attack affected large organizations worldwide even though a patch and so a very convenient counter measure was published nearly a month before.

The cloud-based, open simulation environment enables the participating companies to collaborate in spotting and analyzing risk scenarios. This enables the parties to predict and avoid security risks. Furthermore, the MITIGATE system allows the users to conduct a risk assessment not only of their own specific IT infrastructure, but also of associated, interdependent IT infrastructures in maritime supply chains, as they contain the possibility of spreading threats in cascading effects.

The MITIGATE system already contains a huge number of digital assets and also provides exemplary maritime supply chains. For the implementation of the MITIGATE system the user choses from 'libraries' of assets to rebuild his companies IT infrastructure, or the part of it he wants to assess. Making use of the supply chains provided in the MITIGATE system, or easily adapt them, a user can conduct a proper 4-step risk assessment for e.g. an LNG, container, vehicle- or break-bulk scenario in a short time:

- The Threat Analysis illustrates the overall threat scenario and conducts a first threat assessment by identifying individual cyber threats
- The Vulnerability Analysis describes all relevant kinds of vulnerabilities of the chosen supply chain service and assesses individual as well as cumulative vulnerabilities
- Individual and cumulative impacts on the defined assets are estimated in the Impact Analysis. A possible diffusion of the impact along the supply chain and through the partnering networks is considered
- The Risk Estimation does the same with a view to the specific assets and shows how possible attacks may influence and cause malfunction of single assets and their possible infection amongst each other

The Mitigation Strategy ends the analysis of the risk assessment by providing a risk mitigation strategy. The result shall ensure that all relevant risks in a specific supply chain service are covered.

The MITIGATE system enables even small businesses to have an easy-to-use but effective risk management system that can be used to detect real-time threats from the cyberspace in a timely manner. The software is developed as a cloud solution with the possibility to install it in a company-owned, private cloud; however, the users have their own protected areas available, which are not accessible to other participants. The implementation phase for external partners allows maritime companies to get to know and help the team to test and enhance the MITIGATE system.

ABOUT THE AUTHORS

Dipl.-Ing. Claudia Bosse works as a scientific researcher in the maritime branch of Fraunhofer, after ten years in logistics consulting companies. Her main interests cover developments in maritime transportation and operations trends, especially in the Baltic Sea Region. Since 2015 Mrs Bosse has been part of the MITIGATE project team.

Dipl.-Wirt.-Inf. Martin Stamer works as a scientific researcher in the maritime branch of Fraunhofer after gaining experience in the field of IT consulting and software development. His main interests cover IT management, IT security, and digitalization.

ABOUT THE ORGANISATION

The Fraunhofer Center for Maritime Logistics and Services develops and optimizes processes and systems along the maritime supply chain. Within practically oriented research projects CML supports public and private sector clients of port operations as well as from the logistics services industry and from the shipping business.

ENQUIRIES

http://www.mitigateproject.eu/