

# BETTER CYBERSECURITY

## FOR PORT COMMUNITY SYSTEMS

Dr Nils Meyer-Larsen, Project Manager,
The Institute of Shipping Economics and Logistics (ISL)

Maritime transport is of central importance for the global economy. In order to ensure the smooth flow of cargo through the seaports, electronic data transmission systems for ports, commonly known as Port Community Systems, are used. Port Community Systems are centralized information and data hubs for ports, integrating and distributing information from various sources for global supply chains. They connect companies and authorities involved in maritime transport, such as shipowners, freight forwarders, terminal operators, carriers, and authorities like customs, in particular by providing interfaces to their systems.

Major disturbances for large ports will most probably lead to negative effects on maritime supply chains. In that way, Port Community Systems must be regarded as critical infrastructures – successful cyberattacks can lead to problems for port operations, in extreme cases even a standstill, and – depending on the duration – to bottlenecks in the supplies to industries alongside severe consequences for the whole economy. The recent case of the NotPetya attack on Maersk, which caused some central systems to be down for several days worldwide, is estimated to have caused a loss of about US$200-300 million.

This paper describes first insights into intermediate results of the PortSec research project. This project, funded by the German Federal Ministry of Education and Research (BMBF), uses a software-centric approach in order to detect possible vulnerabilities in cyber security for Port Community Systems. Project partners are the University of Bremen, IT security provider Datenschutz Cert, the Institute of Shipping Economics and Logistics, and DBH Logistics IT, the Port Community System operator of the Bremen, Bremerhaven and Wilhelmshaven ports.

The objective of PortSec is to develop systematic and comprehensive IT risk management protocol in port telematics, taking into account the underlying software architecture and including legal and economic security requirements. The software-based approach focuses on the prevention of attacks rather than their detection and defence. This approach is particularly innovative and has not yet been applied in existing procedural models and standards for the establishment of information security management systems (ISMS). One goal of the project is to develop an industry-specific security standard to prevent cyber attacks. This standard includes a certification scheme for Port Community Systems.

A new sector-specific security standard for cybersecurity of Port Community Systems, compatible with the German IT Security Act, will consider existing regulations and standards like ISPS regulations, and will be developed by PortSec partner Datenschutz Cert and validated by the German Federal Office for Information Security. After successful validation, Datenschutz Cert plans to publish the standard

### THREAT ANALYSIS

Until few years ago, ports were mainly concerned about physical security. However, nowadays the highest risk lies in cyber attacks. Unlike conventional attacks, cyber attacks can be performed

anonymously from a safe distance, possibly thousands of miles away. Attackers can monitor systems and collect information in order to detect vulnerabilities before performing an attack. In contrast to physical attacks, the detection of a cyber breach is far more difficult. Many respective cases even remain undetected. Another problem concerning lacking cyber security awareness is the fact that attacked companies refrain from reporting attacks, as they fear reputational damage.

With regard to the analysis of potential threats, scenarios are developed describing possible cyber attacks on Port Community Systems. For this purpose, the domain-specific business processes in the area of port communication are analyzed. The security requirements of the processes and the processed data are assessed as well, aiming at identifying possible weaknesses, primarily related to interfaces used for communication via the Internet. In addition, the systems are examined regarding protection factors like availability, confidentiality and integrity of data.

Based on the results of the threat analysis, relevant attack scenarios will be defined, and associated economic and business risks will be evaluated with regard to potential damage. For this purpose, each individual scenario will be assessed with regard to the probability of occurrence, vulnerability and consequences in order to evaluate the effects and resulting damage of possible attacks on the Port Community System operator, the port industry, and downstream logistics processes. The impact of attacks and resulting effects on the economy will be examined as well. Previous similar attacks will be analyzed in order to complete the picture of the threat scenarios.

## LEARNING FROM PAST EVENTS

Ports are subject to cyber attacks initiated by different groups, on an almost regular basis. The first group is criminals, aiming to make money out of cyber attacks. In general, criminal organizations are increasingly using cybercrime to facilitate and prepare cargo theft or smuggling based on container-related information. Besides information on the containers' contents, criminals are, for instance, also interested in truck drivers' habits like regular routes and usual truck stops. Criminal organizations are able to use this information to identify the most vulnerable point in the supply chain to increase the effectiveness on their physical attacks. Next, criminals could also encrypt data of port systems in order to extort a ransom fee from the port operator to get access to its productive data again. The second group is commonly known as hacktivists, who are

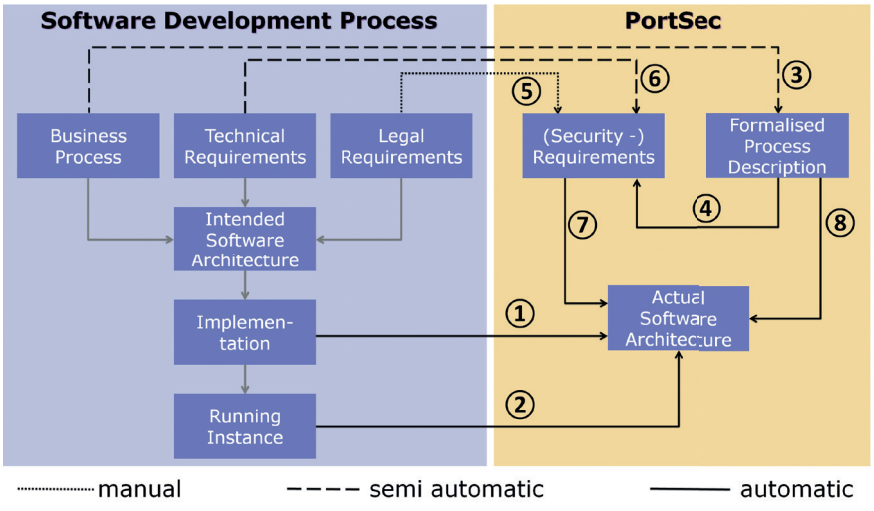


Figure 1: Individual steps of the PortSec approach.

mainly interested in proving their abilities by detecting vulnerabilities in the systems of IT operators which could lead to major disturbances in port operations. The third group is related to corporate espionage and business competition.

Reports indicate several attacks on ports and Port Community Systems' cyber security. A famous incident happened in Antwerp between 2011 and 2013. Hackers were recruited by an organized crime group who hid narcotics in containers used by legal shippers to get access to the drugs later, the recruited hackers accessed the Port Community System of the Port of Antwerp to retrieve the locations and security details of these containers, which enabled the criminals to send their own drivers to pick up the containers before the legitimate owner arrived. At the beginning, the hackers used malware to access the IT systems. After the discovery of the malware, they broke into the port premises and installed key-logging devices on computers.

In another case, cargo system operated by the Australian Customs and Border Protection was penetrated by a crime syndicate in 2012. This syndicate also used legal transports by legitimate shippers for their drug smuggling. Due to the penetration of the system, the criminals were able to check whether these containers were classified as suspicious by police or customs authorities. The crime syndicate abandoned containers which were classified as suspicious.

In March, 2017, the Port of Vancouver in Canada was subject to a Denial-of-Service attack. According to the port's spokesman, the port regularly experiences this type of attack. In contrast to previous incidents, this attack was initiated from inside the port by a virus which infected a computer in the port's network.

These are only a few incidents which were reported to the public. According to the German Bundeskriminalamt, German Police in 2016 investigated a total of 83,000 cases of cybercrime, resulting in a damage of more than $59.5 million (€51 million) in Germany alone. Nevertheless, the number of unreported cases is estimated to be high.

## AUTOMATED TESTING OF SOFTWARE

A comprehensive review of the IT security risks related to software has to identify basic security issues, e.g. with respect to software architecture, lack of encryption, incorrect authorization testing, and unprotected entry points. In particular, the architectural risk analysis must be based on the actual software implementation, and not only on abstract descriptions, which are often incomplete. Since manual architectural analysis is complex and requires considerable expertise, this step should be supported by tools. Therefore, the PortSec project is based on a software-centric approach in which IT security risks are derived from the implemented software architecture in an automated way. Figure 1 presents the individual steps of the planned approach.

First, the implemented software architecture is automatically extracted from the source code of the Port Community System, employing static and dynamic program analyses (1). This step is necessary, since Port Community Systems in general consist of legacy software, which often lacks exact and up-to-date architectural descriptions. The software architecture analysis enables the identification of fundamental security risks for the software with regard to possible cyber attacks. The redesigned software architecture is then supplemented by descriptions of the network in which the Port Community System is operated (2). The network infrastructure is thereby detected automatically.

To consider specific security requirements

of Port Community Systems, the business processes and corresponding legal and business requirements are formally represented (3). As a result, a security evaluator can uncover situations in which unauthorized access to restricted business processes is possible and organizational control rules are circumvented (such as task separation or the four-eye principle). This step ensures that the security requirements are in accordance with the legal and organizational requirements applicable to the operation and utilization of Port Community Systems. The security requirements to be tested are derived from the formal descriptions of business processes (4), legal / economic requirements (5) as well as technical requirements (6).

In the next step, the actually implemented system and software architecture is evaluated with respect to the security requirements and actual business processes. This step leads to the identification of specific risks for port telematics, including the possibility that an employee without authorization can change the declaration of dangerous goods containers due to excessive access rights? At the same time, more general technical security risks are identified, e.g. insecure use of software frameworks or incorrect encryption.

## INDUSTRY-SPECIFIC SECURITY STANDARD

IT Security Act, the German law for the security enhancement of information technology systems in force since July, 2015, reflects the German Federal Government's efforts to considerably improve the cyber security of Germany's digital infrastructures. The IT Security Act allows operators of critical infrastructure and their associated industries to define branch-specific security standards together with the German Federal Office for Information Security (BSI). Building on the results of the PortSec research project, a sector-specific security standard for Port Community Systems will be developed supporting the IT security law and ensuring compatibility with comparable and supplementary standards.

The development of normative controls, which - similar to Annex A of ISO / IEC 27019 - are an addition to an existing ISO / IEC 27001 certification - is planned. The security standard to be developed is being discussed and coordinated with relevant stakeholders in the field and the German Federal Office for Information Security as the responsible agency in accordance with the IT Security Act.

Furthermore, relevant industry associations will be involved in the activities.

The industry-specific security standard to be developed consists, on the one hand, of an audit scheme which defines the scope, depth and methods of testing.

On the other hand, the security standard includes a certification scheme which specifies the processes for a multi-stage certification process and defines the life cycle of certificates, auditors and test bodies. This is particularly important as the IT Security Act requires all critical infrastructure operators to provide a proof of compliance with all requirements, explicitly calling for security audits and certifications. Within the framework of PortSec, an audit and certification concept will be developed, which can be used by all kinds of operators of critical infrastructures in the area of maritime transport.


## ABOUT THE AUTHOR

Dr Nils Meyer-Larsen is Project Manager at the Institute of Shipping Economics and Logistics (ISL) in Bremen/Bremerhaven, Germany, and leader of the ISL competence area "Maritime Security". He studied Physics at the University of Hamburg and obtained a PhD degree in Physics. Nils Meyer-Larsen has managed several national and international research and development projects in the fields of maritime transport and supply chain resilience as well as satellite-based services for the maritime industry. Furthermore, he works as a lecturer at the Bremerhaven University of Applied Sciences in the Master's degree course Integrated Safety and Security Management.

## ABOUT THE ORGANIZATION

The Institute of Shipping Economics and Logistics (ISL) is an independent, not-profit making research institute founded in 1954 located in Bremen and Bremerhaven, Germany. ISL is one of the leading maritime research and consulting institutes in Europe. Around 40 employees work together in interdisciplinary project teams, well equipped with modern instruments in practice-oriented research and development projects. Together with its partners in the MarSat network, ISL works towards creating and integrating innovative satellite-based services for the marine and maritime community.

## ENQUIRIES

Email: meyer-larsen@isl.org
Website: https://www.isl.org/en