KR Maritime Cyber Security

News from KOREAN REGISTER

Nov 2018

Vol. 007

KR Cyber Security Activities

● Cyber Security Training to Maritime Industry

Last October, KR Cybersecurity TFT conducted 'Understanding of Maritime Cyber Security' and 'Maritime Cyber Security Management Practices' as training of Consortium for HRD Ability Magnified Program provided by KR Education & Training Center.

'Understanding of Maritime Cyber Security [8H]' aims at improving understanding of cyber security for executives, employees and seafarers in maritime industry (Shipping company, shipbuilder and equipment company) and raising awareness of maritime cyber security through training on cyber security organization, cyber asset management and threat, human & physical & technical security required for cyber security.

'Maritime Cyber Security Management Practices [16H]' is the advanced training consisting of Cyber security IT explanation and practices and cyber risk assessment understanding and practices. In particular, through risk assessment workshops, cyber vulnerabilities of company and ship can be identified, and procedures and methods of risk assessment, and improvement measures can be identified directly.

Through these trainings, Korean Register provided training for improving awareness of cyber security required for IMO and OCIMF's TMSA/SIRE and RIGHTSHIP inspections and method how to perform cyber risk assessment to domestic maritime industry. And various cyber security practical trainings reflected feedback will be held in 2019.

● Technical Seminar 2018 in Rep. of Turkey and Greece

Korean Register held KR Technical Seminar 2018 and 13rd Hellenic Committees on maritime industry in Rep. of Turkey and Greece from Oct. 30 to 31. More than 50 people attended seminar in Turkey on Oct. 30, and more than 100 people from shipping companies, shipbuilders, and academia attended seminar in Greece on Oct. 31. At the seminar, Korean Register presented trends of BWMS, the latest bulk carriers hull, practices of cyber security, and SOx regulations. In particular, it was shared to stakeholders that the proposal to introduce a sulfur dioxide experience building phase was suspended at IMO MEPC 73. It relieved the curiosity of stakeholders about enforcement of ship sulfur dioxide regulation. And the 13rd Hellenic Committee of Greece was held in Athens, Greece on Nov. 1. 60 committee members from related industries including major shipping companies in Greece and the region near Greece discussed the latest major issues in the maritime industry. In this committee, Stephen Gordon, executive of Clarkson Research, presented the current status of the maritime business, which received the attention of many participants.

President Lee of Korean Register said "Currently, the maritime business is in a chaotic situation due to strengthening environmental regulations and uncertain future. In order to contribute the maritime industry, Korean Register will continue to provide information on the latest trends."

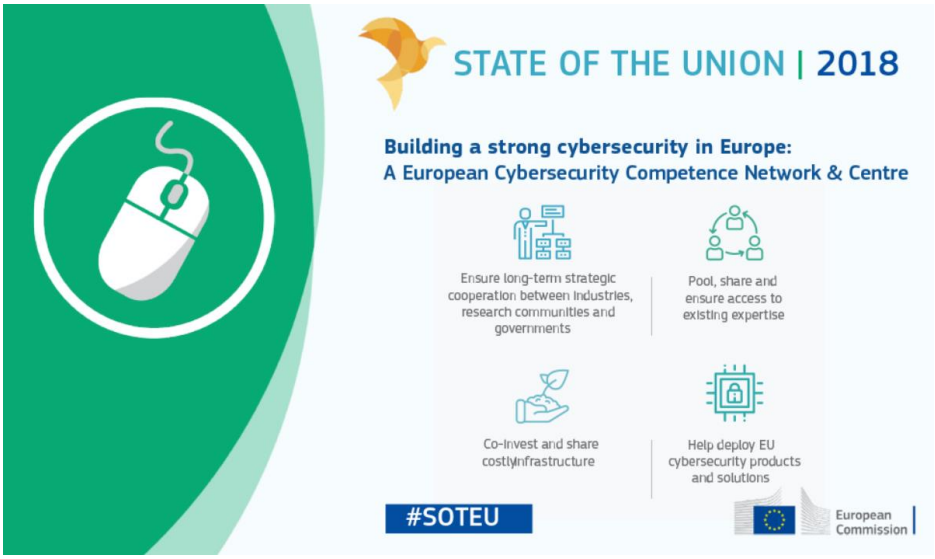
Establishment of EU Cyber Security Certification Framework

- **Establishment of EU Cyber Security Certification Framework**

To improve cyber resilience, EU is building a certification framework for ICT products, services and processes. On June 8, 2018, the board od directors agreed to a proposal(Cyber Security Act) to complete the TEXT through negotiation with the European Parliament. One of effects of this proposal is that the current EU Network Information Security Agency(ENISA) will be upgraded to a more stable EU agency for cyber security.

- **Certification of Cyber Security**

The proposed certification framework provides an EU-wide certification regime as a comprehensive set of rules, technical requirements, standards and procedures. Certificates issued under the that plan are legally recognized throughout the EU, and this certification demonstrates that ICT products and services comply with specified cybersecurity requirements under the plan. Thus, certification means that the technology has received a European cybersecurity stamp and enables companies to do business across borders. Currently, the regulation was approved by the EU Commission and is expected to be formally introduced like the GPDR if passed by the European Parliament.



Ref. : The EU cybersecurity certification framework

Nigeria Hacking Group launched a maritime cyber attack

- **Cyber Security issue in Maritime Transportation**

Cyber security threats in the maritime industry are also growing as ICT (Information Communication Technology) is applied to domestic and foreign shipping systems, port management and operation, and autonomous navigation ships. Organizations that make cyber attack on maritime industry are constantly discovered and they used various type of cyber attacks such as e-mail compromise, e-mail spoofing, advanced persistent threat, spear phishing, physical takeover, etc.

In particular, threat range from physical factors, which were frequently mentioned in existing physical security such as piracy, lost cargo, smuggled ports, shipwrecks, and so on to hacking into IoT(Internet of Things) applied newly-reviewed smart ship, embedded system and various cyber assets is expanding.

In the case of Gold Gallon Hacking Group in Nigeria, which occurred in April of this year, it is an example of cyber crimes committed by shipping companies only, and in the case of related hacking incidents, the E-mail information takeover of domestic shipping companies was also included.

- **Cyber attack cases by Nigeria hacking group**

The shipping industry is highly vulnerable to Business E-mail compromise(BEC), Business E-mail Spoofing(BES), fraud and other cyber attacks. Due to industry characteristics, workplace are spread around the world and depend heavily on satellite communication services via V-SAT, FBB, F33 and F77. In addition, information sharing with the central or head office does not occur frequently compared to other industries except for safety sectors. This is why security accidents referred to as high-level personnel of the headquarters occur frequently.

Ref. : DarkReading

Gold Galleon's offensive strategy and techniques are not very new or sophisticated. However, they only select the attack target well and seek the vulnerability. They infiltrate the company's systems before the actual attack and steal related information such as internal and account contacts, ship schedules, and payments. Then, they carefully analyze the company's website, which is targeted, and use it for fraud in conjunction with pre-picked information. In other words, they use spear phishing via e-mail. At this point, malwares like Predator Pain, PonyStealer, Agent Tesla and Hawkeye are transmitted along with payload.

Betke, analyst at Secureworks Counter Threat Unit, "Gold Galleon distributes the Malware loader during a spam attack that doesn't have very high volumes. If the data is then successfully accessed, they review the data to check the shipping status and shipping schedule. In particular, they identify the dates associated with receipts and invoices, and intercept the PDF file in the form. Then they send it back by slightly changing the recipient's address. It's actually a simple fraud. They know all the schedules of ships and shipments, and the fake bills they send are for stealing real forms and manipulating only a fraction of the information, so company usually has to be fooled."

Response and Suggestion

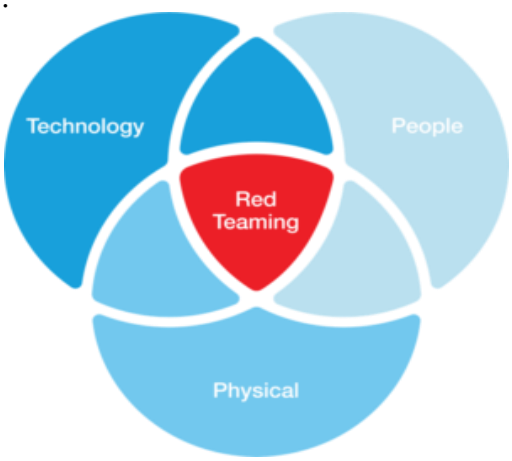
The shipping industry delivers 90 to 94 percent of the world's trade volume, where large amounts of money and data are exchanged with stakeholders, but security is limited to physical parts. In a survey of marine industry officials including seafarers, 21 percent said yes when asked if they had been victimized by cyberattacks. They also answered that the damage was due to a functional problem with IT systems (67 percent), loss of company data (48 percent), financial loss (21 percent), and problems with maritime transport systems (4 percent). Training of employees, setting strong passwords, encryption, and introducing dual authentication are recommended ways to prevent this.

What are O/T assessment and Red Teaming project?

- **Need of O/T assessment and Red Teaming Project**

Although security checks for ports and ships can take place in several forms, Red Teaming projects that perform security checks in the OZ (Operation Zone) are recommended based on understanding of the site and related industries.

Red Teaming evaluations focus on providing security teams within the company with real-world experience in response to cyber attacks in the OZ area as well as on actual IT. While this security assessment service is used for avoiding attacks that harm the company's physical operating systems or business, it uses traditional and intelligent attacker tactics and Techniques and Procedures (TTPs) to target the objective prepared by Red Teaming Project and company security team.



As shown in the figure above, physical penetration is carried out through understanding of the actual operating environment beyond the security diagnosis of existing technology areas, as well as attacks on internal employees (including maritime engineers) working on land and sea using social engineering hacking.

When an applicant sets an target(business scenario assuming the worst case scenario), it starts Red Teaming work provided by security companies. Finally, Red Teaming implements the entire attack life cycle from initial reconnaissance

to mission completion.

Attack forms begin with an understanding of the operating environment for ports and vessels. Based on this, Red Teaming defines the most important assets of the applicant and sets the project's goal through consultation with the applicant.

Red Teaming activities test the ability of the applicant's internal security personnel protecting the most critical assets. Based on his experience at the forefront of cyberattacks, the expert simulates TTPs (tactics, techniques and procedures) of actual target attacks without harm.

Red Teaming operations are appropriate for organizations to test their ability to protect critical assets from targeted attacks. Red Teaming security activities are appropriate for organizations that want to train their security teams to improve infringement detection and response against targeted attacks.

Given that an attacker starts understanding the operating environment for ports and ships, we should think about the basic requirements for the officer responsible for security with the appropriate security team.

Before specific handling of Red Teaming activities, security in the ICS/SCADA area will be serialized to address Operation Zone security.

- **This article was written by Lee Seung-jun, senior researcher at NSHC & Shield Consulting co., Ltd.**

NSHC SECURITY, the only cyber security company in Domestic and Asian that can carry out penetration testing of ICS/SCADA(OT), is conducting malicious code analysis such as ransomware and APT attacks, penetration testing of industrial devices and source code diagnosis.

SHIELD CONSULTING is providing consulting on physical security(CCTV, control of outsider's access, control of electronic devices and locks) required in cybersecurity.

Understanding of Cyber Threat

- **Understanding of cyber threat**

A Cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service (Source: NIST SP: 800-128).

Cyber threats need to be categorized periodically to identify vulnerabilities of assets as their impact on the asset changes as ICT technology evolves.

- **KR Guidance for Maritime Cybersecurity Management System requirement (CSMS1)**

204.1 Risk Management : External environmental factors affecting the environments of internal information technology and operational technology should be identified and cataloged as threats.

- **BSI top 10 cyber threat**

Threats to ICS are activities or events that could potentially cause damage to ICS and its related businesses due to existing vulnerabilities. The following table lists the most serious threats to ICS published by the German Federal Information Security Agency. Following the newsletter in July, we will analyze the "Technical Malfunctions and Force Majeure" of the BSI 10 cyber threats.

- **BSI top 10 cyber threat : Technical Malfunctions and Force Majeure**

Hardware defects and pure operational errors can occur in security-related system components and ICS components that can cause unexpected malfunctions. And software errors cannot be ruled out either in that system components. In particular, hardware defects are more likely to occur in certain

scenarios due to existing environmental conditions (dust, temperature, etc.) unless necessary precautions are taken.

<Potential threat scenarios>

- ❖ System component defects, such as hard disk failure or network switch failure, cable breakage, etc.
- ❖ Hardware faults and errors in software components can remain undetected for long periods of time. (For example, system restarts or certain restrictions may apply)
- ❖ Software errors can cause the system to malfunction. For example, restarting the system after updating the operating system of the central security component can cause malfunctions. This scenario can occur not only through insider trading, but also through carelessness and human error. In particular, these incidents can greatly limit availability due to organizational shortcomings.

<Countermeasures>

- ◆ Establish business continuity management, including aspects such as potential countermeasures, system recovery procedures, alternative communication options, and training implementation.
- ◆ Prepare an exchange or replacement device.
- ◆ Patches, updates, and new software components must be thoroughly tested before installation on the operating system.
- ◆ Important components should be designed with a redundancy concept.
- ◆ In order to select the systems and components to be used, sufficient minimum requirements must be defined and enforced in accordance with the identified protection needs. Some important aspects are:
  - Reliability of the product supply chain
  - Product robustness
  - Existence of appropriate security mechanisms (e.g., security authentication)
  - Long-term availability of spare parts, updates and maintenance
  - Appropriate availability of patches
  - Do not use unnecessary functions of the product

Ref. : Industrial Control System Security – Top 10 Threats and Countermeasures 2016

Guide to Building the Personnel Security System

- **The need for establishing personnel security system**

The purpose is to protect the cyber assets of the company and the ship from various type of threats by establishing procedures for hiring, contracting and transferring employees, cyber security training, and punishment of cyber security offenders. Personnel security system applies to all employees (full-time and contract workers) and external personnel (dispatched workers, subcontractors, etc.). Non-Disclosure Agreement (also known as a confidentiality agreement) must be made in written and signed to be effective.

- **KR Guidance for Maritime Cybersecurity Management System requirement (CSMS1)**

Security Training (203.1) : The personnel involved in security activities should conduct security training at least once a year in accordance with the security training plan.

Security Training (203.2) : Security training for new employees (including contractors and temporary workers) and retirees should be carried out. In particular, training should also be provided for domestic and overseas business travelers and absentees.

- **Confidentiality Agreement (Non-Disclosure Agreement)**

1) The newly hired or transferred personnel shall sign and provide to the company a written agreement stating that the handling of company's important information, the necessity of cyber security , and responsibility..
2) At the time of retirement and transfer of employees, an employee confidentiality agreement shall be made to prevent leakage of important information of the organization and remind them that they have legal responsibility for leakage.

3) When a temporary worker or an outsourcing contractor is granted access to information assets, a confidentiality agreement must be signed that includes the obligation to comply with cybersecurity requirements and any claims for damages in the event of a cyber incident due to non-compliance.

4) If personal information is included in the agreement, it should be kept in a physically safe place to prevent leakage to an unauthorized third party.

- **Outsider Security**

In case of using outside workforce and outsourcing service, if security management is neglected, cyber incidents may occur due to personnel security vulnerability. Therefore, it is necessary to check beforehand whether or not a confidentiality agreement is written, and all of the computer equipment can be brought in / out after approval by the security officer. Work PCs should be blocked from accessing the harmful sites and it is necessary to check whether there is possibility of leakage of important information when carrying them out.

- **KR Guidance for Maritime Cybersecurity Management System requirement (CSMS1)**

Outside Parties' Security (209.1) : The company shall establish a security policy for information technology equipment and data of outside parties in order to prepare for security incidents by the outside parties.

Outside Parties' Security (209.2) : The company shall specify the security requirements, management and supervision during the project period when contracting with outside parties.

Outside Parties' Security (209.4) : The outside parties shall use the system in compliance with company security requirements and perform the security function check before connecting the equipment owned by the outside parties to the system.

Explanation of term

- **GDPR :** In May 206, EU enacted the General Data Protection Regulations, which ensures the free movement of personal information between EU members and strengthened the right to protect personal information in a digital single market. It went into effect on May 25, 2018. Unlike the existing Directives, GDPR itself has direct legal binding on all EU member states and imposes heavy sanctions on companies that violate GDPR. (Penalty: 4% of global sales or 20 million euros)
- **Spoofing :** This refers to a technique in which malicious network intruders attack other target systems by cheating their own identification (IP address, DNS name, MAC address, port). An attacker constructs random websites to induce visits by general users, obtains user system privileges using the architectural flaws of the Internet protocol, TCP/IP, and steals information or IPs granted.
- **Spear Phishing :** This refers to E-mail or electronic communication fraud attempted against a specific organization, primarily aimed at obtaining information from accessing confidential data by unauthorized users. Spear phishing is performed for monetary or for trade secrets and military information rather than for random by ordinary hackers. To prevent Spear Phishing, The user has to make sure to check the sender accurately, check the response URL for reliability, and avoid providing his/her important personal information, such as passwords.
- **Scam :** This refers to a criminal method that intercepts trade transaction payments by hacking into corporate e-mail information and pretending to be a client. After infecting targeted company with malware, the attacker induces the company to change their payment method. Scammer monitors what trading partners communicate by hacking e-mail and in case that there is transaction, sends fake account information as if the major partner sent e-mail and withdraws the transaction amount.