PORT AND SHIP CYBER SECURITY

AFTER 'NOTPETYA'

Phil Tinsley, Maritime Security Manager, and Aron Frank Sørensen, Chief Marine Technical Officer, BIMCO, Bagsvaerd, Denmark

The maritime industry has awoken to the potential impact of cyber security incidents on ship operators, ports and the industry as a whole. The well-publicised July, 2017 NotPetya ransomware attack on a number of reputable companies, including Maersk and its ports subsidiary APM Terminals, has highlighted not only the industry's cyber-vulnerabilities, but also the increasing sophistication of the methods used in the attacks.

To understand this event, it is important to recognise that the flaw in any operating system's secruity may be found not just the technology behind the operational system, but also in the individuals who operate the systems.

The NotPetya attack targeted computers running Microsoft Windows operating systems and was designed to spread across closed organisational networks by exploiting administrator privileges. This allowed it to spread quickly with relative freedom across multi-national companies.

Hackers try to exploit the fact that individuals are often unaware of cyber attacks and forget to use common sense on the computer. BIMCO believes that there is an urgent need for a holistic approach to be applied in every organisation, to ensure that every individual is fully aware of the dangers and knows how to mitigate them. Putting a robust system in place, the organisation can prevent, detect and better recover from cyber attacks.

Internationally the industry has recognized the urgent need to raise its awareness of cyber risk threats and vulnerabilities. The IMO in 2017 adopted guidelines on maritime cyber risk management, which includes ports. These guidelines provide recommendations on maritime cyber risk management to safeguard shipping from cyber threats and vulnerabilities.

In addition, The Guidelines on Cyber Security Onboard Ships was launched in July, 2017, a revision of the first publication which was introduced to the industry in January, 2016. The document is a collaborative effort by major industry representatives including BIMCO, various ship owning entities, Maersk Line, Chamber of Shipping of America, International Union of Maritime Insurance, and the United States Maritime Resource Center. The advice is predominantly aimed at shipowners but also ports operators and is regularly reviewed to reflect industry requirements and new developments in each sector.

The second edition is fully aligned with the IMO's guidelines and includes information on insurance issues and how to effectively segregate networks. It also provides practical advice on managing the ship to shore interface, and handling cyber security during port calls and when communicating with the shoreside. It covers contingency planning and responding to, and recovering from, cyber incidents. Some aspects of the guidelines are aimed specifically at ships.

Cyber risk management must be initiated at a senior management level of a company because it will impact both business procedures and operations, it will incur costs and timelines may need to be set for the training of personnel roll-out of technologies. This essential training does not need to be high level. A combination of campaigns to raise awareness of potential breaches and easily followed guidance on reporting suspected cyber-attacks can be easily delivered and is a good staff skill enhancement option.

The recent NotPetya attack was a classic security breach as opposed to an attack on operational safety systems, as leading global transport and logistics operator Maersk admitted that "multiple sites and business units" had had to be shut down after the cyber attack.

It's now clear that the NotPetya was a "wiper", and not ransomware. The earlier version of the Petya virus had encrypted a disk and demanded a ransom, while the reconfigured NotPetya was designed to cause maximum chaos. NotPetya demanded a ransom but there was little mechanism to collect funds and the virus destroyed the disk regardless.

Any ship or port cyber security strategy begins with identifying the threats to the ship or port. These could be internal threats posed by inappropriate use of technology, or they could be external threats.

This strategy must include actions to identify system vulnerabilities within vessel systems with direct and indirect communication links to the shore. The consequences of cyber security threats to any system must be understood and measured against existing protection measures.

This should be followed by an assessment of risk exposure and measuring risk to determine the likelihood of vulnerabilities being exploited by external threats or internal inappropriate use. The impact of a combination of vulnerabilities being exploited at the same time should also be determined.

The port or ship should then develop protection and detection measures to reduce the likelihood of vulnerabilities being exposed and reduce the impact of a vulnerability being exploited. Contingency plans will be needed to reduce the impact of threats on the safety and security of the ship or port. Being able to respond and recover from cyber security incidents through the implementation of an established response plan, allows a further opportunity to assess the effectiveness of the response plan and to re- assess the threats and vulnerabilities.

Modern technologies such as automated management system controls can create vulnerabilities for ships and ports, particularly if there are any insecurities in the design of the organisation's network or uncontrolled access to the internet. Additionally, shore side and onboard personnel may not be aware that some equipment producers maintain remote access to shipboard equipment and its network system. The risks of misunderstood, unknown, or uncoordinated remote access to the network system of an operating ship should be taken into consideration as an important part of any risk assessment.

It is recommended that both shipping companies and port operators ensure that they fully understand the ship's OT and IT systems and how these systems connect and integrate with the shore side. Some of these systems connect directly to the port operations, so it's necessary to appreciate how any safety, operations, and business activities might be compromised by a cyber incident both at the port and onboard. Hackers will search for and target the weakest link in the chain and concentrate their attacks there.

Visitors to ships in port can connect the ship to shore in other ways too. It is common for technicians, vendors, port officials, marine terminal representatives, agents, pilots, and other technicians to board the ship and plug in devices, such as laptops and tablets. In such cases, these visitors must be aware of the cyber risks of doing this.

In an effort to raise awareness onboard and in ports, posters could be promulgated to remind individuals of potential dangers. Simple messaging will promote alertness and encourage individuals to ensure they are not in breach of any cyber control policies.

Ships and port operators can learn from the experiences of others and work together to ensure that sufficient protection is in place. This would be made considerably easier if the industry shared incident information and best practice. Unfortunately, such a system of collaboration does not currently exist. At the moment, we have evidence that shipowners and port operators are having to manage cyber security incidents fairly frequently, but until the industry as whole shares its experiences, there is little potential to learn and protect against a major breach in the future.

ABOUT THE AUTHORS

Phil Tinsley is a former officer in the Royal Marine Commandos, attaining the rank of Major after 31 years military service. His military career included littoral operations on a global scale, warfighting and specialization in cold weather warfare. at Since leaving in 2010, Phil has managed offshore security in the Indian Ocean High Risk Area in support of seismic operations, which included two Somali pirate attacks at sea. He went on to establish and coordinate anti-piracy transit operations for a respected private military and security contractor based in Dubai. Phil has a thorough understanding of port operations, personnel training requirements, compliance and management systems. Phil joined BIMCO in 2015 and holds the position of Head of Maritime Security. His primary role is to assist members with all aspects of maritime security; including piracy, drug smuggling, stowaways, mixed mass migration and cyber security. Currently based in Denmark near BIMCO House, Phil maintains his hobby as a cyclist and is always happy to take any queries members may have on any relevant maritime issue.

Aron Sørensen is Head of Maritime Technology and Regulation and is responsible for BIMCO's technical affairs. He manages BIMCO's role relating to marine, operational and related matters at a number of international organizations such as IMO, ISO, IACS and IHO. His tasks include negotiating, monitoring and disseminating relevant conventions and developing international standards, regional/national requirements, and assessing their impact on BIMCO members. He is BIMCO's project leader on developing industry guidelines on cyber security onboard ships (BIMCO, ICS, INTERTANKO, INTERCARGO, IUMI, CLIA and OCIMF), the 2015 BIMCO/ICS Manpower Study, and software maintenance standards (BIMCO and CIRM) which is being tested on board ships in the first half of 2017. Following a career at sea as a deck officer, Aron Sorensen taught apprentice deck officers at Nautical Institutes in Denmark. After some years of teaching he joined the Danish Maritime Authority working with safety of navigation in Danish waters. In 2008 he joined BIMCO.

ABOUT THE ORGANISATION

BIMCO is the world's largest international shipping association, with 2,100 members in more than 120 countries. Our global membership includes shipowners, operators, managers, brokers and agents. Our vision is to be the chosen partner trusted to provide leadership to the global industry. Our mission is to provide expert knowledge and practical advice to safeguard and add value to our members' businesses.

ENQUIRIES

Email: pt@bimco.org
Website: www.bimco.org