KYND

Cyber risks in the maritime industry

With approximately 90% of world trade carried by sea, the maritime industry has quickly become an attractive and lucrative target to opportunistic cyber criminals, especially as the sector involves and heavily relies on a multitude of participants in the process – ports, logistics firms, intermodal transport companies – to deliver valuable cargo around the world.

With the speed of innovation rapidly increasing, industries are looking for new ways to become more agile, productive and to stay ahead, and maritime is certainly no exception. Whilst technology adoption contributes directly into improving shipping operations, safety, security, and reducing operational complexities of logistics, it also creates significant new risks, along with its many advantages.

The global maritime industry faces a constantly increasing number of cyber threats, stemming from the sector's critical reliance on advanced technology (such as fully automated ships, smart shipping, energy management solutions) to the growing actions of cyber criminals challenging the sector with malicious intent. Cyber-attacks in the maritime industry could result in the compromise of sensitive data, loss of life and physical assets.

Business exposure and implications

Access to organisations' confidential information

Phishing campaigns remain the most preferred method of attack for gaining access to sensitive areas within an organisation's network, including systems and data. Such scams can lead to significant problems to maritime organisations with far-reaching impacts, ranging from unauthorised access to cargo management systems, monetary fraud or even hijacking of vessels and crew members.

The threat of AIS signal spoofing

Automatic Identification Systems (AIS), a key navigation tool for the maritime industry that is used for vessel positioning and tracking, are not protected by sophisticated encryption or authentication, therefore, are highly vulnerable to spoofing attacks. Transmitting false AIS signals can be used by cybercriminals to impede vessel tracking, create false navigation obstacles, cause collisions and create untraceable attacks.

Bring-your-own-device (BYOD) vulnerability

Driven by the need to increase efficiency whilst reducing costs, many maritime organisations adopt a ''Bring-Your-Own-Device'' policy on their vessels allowing for these devices to connect to networks without being adequately configured, therefore further exposing the network that is linked to critical systems and valuable data to contracting malicious content.

The legal implications and reputational damage

Failure to adequately protect clients' confidential information in case of a data breach can not only cause reputational damage, loss of clients and reduced business profitability, but also lead to substantial GDPR fines and penalties that can adversely affect the business.

Supply chain cyber risk

With over 90% of the world's trade carried by sea, cyber-attacks represent an enormous potential threat to international trade capabilities. And with all the intermediaries involved in shipping, the risk applies to not only the maritime organisation themselves, but to all involved in the shipping process. The impact caused by a cyber incident to any of those involved could be huge.

Key industry statistics

91%

of ship security officers surveyed said they didn't have the training, knowledge or skills to deal with cyber threats[1]

$300m

is the cost of lost revenue to Maersk in 2017 as a result of the ''NotPetya'' destructive cyber attack[2]

4.2

the average amount of new files of malware code being generated every second in 2017[3]

900%

rise in the number of reported operational technology (OT) cyber incidents in the maritime industry over the last three years[4]

What types of risks exist?

There is a variety of different threats that the maritime industry could be impacted by, but the most common include:

Phishing
Malicious emails designed to look like genuine emails which encourage employees to click – infecting their computers or stealing passwords in the process.

Viruses
Code which infects computer systems, corrupting or deleting data.

Hacking
An individual or group attempting to gain access to company systems with the intent to steal or destroy data.

Ransomware
A malicious programme which locks access to company files and data until a ransom payment is made, after which time access may be restored.

Case Study

Type
Vessel's administrative systems infected with malware after using an infected USB flash drive.

Scenario
A dry bulk ship in port had just completed bunkering operations. The bunker surveyor boarded the ship and requested permission from the team to access a computer in the engine control room to print some documents for signature.

Sting
The documents required for printing were kept on a surveyor's personal USB flash drive which he was using for business purposes. The surveyor inserted the drive into the computer and unwittingly introduced malware into the ship's administrative network.

Investigation
The malware went undetected until a cyber assessment was conducted on the ship later, and after the crew had reported a "computer issue" affecting the business networks.

Conclusion
Global adoption of Bring-Your-Own-Device (BYOD) by all industries emphasises the need for mandatory procedures to have full control over, or restrict the use of mobile devices (e.g. tablets, laptops, USB drives, etc) onboard, including those belonging to visitors.

KYND

KYND's analysis of key cyber risks of the top* 100 world's largest container ports

*by container throughput

Ransomware Risk

16.0% of ports had at least one external internet service exposed which would place them at a higher risk of a ransomware attack.

Email Spoofing

100% of ports were vulnerable to having their email addresses spoofed.

Vulnerable Services

55.6% of ports were running at least one service, such as an email server or web server, with a well-known vulnerability to cyber attack.

Out of Date Software

21.1% of ports had at least one service that was using software which was out of date, no longer supported and vulnerable to cyber attack.

Certificate Issues

37.8% of ports had at least one security certificate which had expired, been revoked or distrusted.

How KYND can help

- With just a website name, KYND reveals your organisation's cyber risks
- Instantly KYND lets you know if your emails are spoofable or if you're vulnerable to a ransomware attack
- KYND provides clear and easy recommendations without using technical jargon
- KYND continuously monitors and alerts you instantly if any new cyber risks are found

Get in touch

✉ broker@kynd.io

🌐 www.kynd.io

References:
[1] https://globalmaritimehub.com/wp-content/uploads/attach_908.pdf, 2017, Global Maritime Hub
[2] https://www.infosecurity-magazine.com/news/maersk-admits-notpetya-might-cost/, 2017, Inforsecurity Magazine
[3] https://www.gdata-software.com/blog/2017/04/29666-malware-trends-2017, 2017, GData Software
[4] https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/, 2020, Safety4Sea