The Nautical Institute

Nautical Institute Cyprus Branch and The Cyprus Master Mariners Association.

Event Report

A WORKSHOP ON CYBER SECURITY

The Nautical Institute Cyprus branch & Cyprus Master Mariners Association hosted a joint event at the Marlow Building, Limassol, on Wednesday 23rd March 2016. The interest in the topic was high, as was evident from the packed venue with 85 attendees. The event was kindly supported by InterManager.

The Chairman, Capt. Graham Cowling welcomed the participants by sharing a recently published news article that cyber-attacks could cost the oil and gas industry billions of US dollars up to 2018. He asked the audience to imagine a 20,000 TEU container ship passing through the the Straits of Malacca and losing the GPS, ECDIS and ship's control systems.

The workshop was conducted by SOFTimpact, a Cyprus based consulting and maritime software development company. The company specializes in products like payroll, crewing, KPI and other business solutions including cyber security.

The main questions were: How vulnerable are the ship based systems such as GPS, ECDIS, GMDSS, the engine and cargo automation systems to manipulation? How about shore office based systems? How can we be prepared to tackle these threats, both internal and external? How can we prepare our crew and offices to be Cyber-Safe?

The first speaker was Markus Schmitz, Managing Director of SOFTimpact.

He described a few recent incidents:

Fraudsters presenting themselves as a known bunker company in Nigeria have stolen EUR 565,000, from a shipping company registered in Cyprus.

USCG issued a GPS jamming attempt – this was achieved using a very simple GPS jamming device in the area.

37% of all Microsoft servers on ship vulnerable to attacks, according to a 3rd party study.

Whereas Markus held the belief that in fact the figure could be much higher

Pirates hacked into a shipping company's cargo management system to identify possible items for theft. This allowed them to board the vessel and open only high value containers over a seven month period before the exploit was found.

Markus stated that most cases are actually phishing scams involving simple emails. Some of the giveaways are that the emails are addressed to a general email, or there is a .gz file extension. Most hacks are in the shore based office and reveal some sort of insider knowledge, possibly obtained by monitoring emails.

On the ship, GPS spoofing and clock skewing are possibilities. With satellite communication system systems, the ‘back-door entry’ made possible by weak password reset mechanisms.

AIS protocol lacks encryption and authentication. This makes it very vulnerable to manipulation.

SOFT impact clearly identified the ECDIS being the most vulnerable of ship systems because they are based on operating systems that can be attacked by virus and malware. The ECDIS systems also support the use of portable media such as USB sticks, which present the biggest danger.

The shipping industry is vulnerable as it carries out business globally and onboard many people have physical access to systems raising the risk that unauthorized devices or compromised devices are plugged into ship systems infecting them and opening them to attack.

Lee Williamson, IT Security Consultant for Cybersail.org then presented an interesting live demo of capturing information on a public Wi-Fi network such as usernames, passwords, credit card details, cvv numbers and other confidential data. This is something seafarers should be aware of when using free wifi in ports for example. In addition he gave examples of how USB dongles can be used to record all key strokes and take screenshots of PCs they are plugged into and how this could leak confidential information from a Masters PC onboard.

What should a company do? The proposed actions were

Establish a Cyber defense strategy.
Include cyber-security in the Ship’s and Company’s security plan
Assess your IT vulnerabilities and risks
Implement suitable security technologies
Cyber defense planning
Train your staff to be security aware
Audit your business partners
Continuously review & define

Markus also announced an initiative of SOFTimpact called Cybersail.org. A community based website dedicated to the topic of Cyber Security for the Maritime industry. The vision is to become the place anyone involved in Maritime can go to learn about Cyber threats, defense and share their experiences.

The event was followed by a snack, drinks and networking session. Feedback from the participants was very positive.