Case study for onboard safety meeting

Cyber security - safety of the crew

Please read the below description of an incident. Keeping your company's standards and vessel procedures in mind while reading to compare with the actions of the crew below. We will discuss the factors which led to the incident occurring and how to avoid it from happening on our vessel.

Background

Across the global maritime community, vessels and their crew are increasingly connected to and dependent on digital systems that makes use of cyberspace (Internet), and thereby exposing them to its risks. Connectivity boosts morale and wellbeing onboard, by enabling crew to stay in touch with company, family and friends, send emails, make phone and video calls, use social media, and read news and download entertainment.

The risk of exposure to cyber threats are higher where antivirus software is not being updated and out of date operating systems are used on computers and devices onboard. Cyber threats are most likely to come from within the ships' network, either from a vendor or the crew's use of personal computers in the form of virus emails, phishing, download of improper content, to name a few. The easiest and most common way for cyber criminals to strike, is through a socially engineered attack, negligence or poorly trained individuals.

When malware is introduced to a computer or ship system connected to the internet, it is common for the malware to establish a hidden communication channel to outside world. The result is possible encryption of the system, unauthorized transfer of data and several other types of serious misuse of personal and company information. These types of communication are not necessarily identified as a threat by antivirus scanning software.

The following is not an actual incident but illustrates how easy it can be to fall victim to a cyber attack.

The incident

A ship on a voyage from Asia to Europe had just arrived at anchorage for a short stay to take on some bunkers, provisions and to undertake a crew change. The Master had already announced that a launch boat was on its' way out and that the signing-off crew had to prepare for disembarkation.

One of the signing-off crewmembers was very happy to finally disembark the ship and to be heading home to his family. Since there was some spare time whilst waiting, he turned on his smartphone and took a selfie of himself showing the ship and the sun setting behind a big skyline ashore. He discovered that there was a free public wi-fi network available and tried to connect to it as he wanted to share the picture he had just taken with his friends on social media and to announce his return home.

To get the internet access, the wi-fi provider required him to enter some information such as email address, ship's name, nationality and home town. He also discovered there would be a higher internet speed provided and even a gift, a t-shirt that could be collected in port, if he would just link his private social media profile to the site by simply entering the social media

account id and password and then click 'ok', which he did. Once online at full speed, he posted his picture on social media and tagged the port at the same time. He then hurried off to the gangway, as the launch boat had arrived.

What the crewmember did not know, was that another crewmember who was not signing off, had done the same and connected his personal laptop to the same wi-fi provider, by registering his social media profile to get the higher internet speed in order to send some files and medical records to a prospective new employer as well as to download some newly released tv-shows.

Neither crewmembers were aware that a small piece of malware had been planted on their device when they pressed the 'ok' button. The malware monitored all the emails sent to and from their devices and shared this with unknow third parties, once the users were connected online. Once the signing-off crewmember arrived home, he wanted to transfer the pictures taken during his recent voyage to his family's home computer. He connected his smartphone to his home computer using a USB cable, and transferred not only the pictures, but also the malware that had been downloaded through the earlier wi-fi connection.

The crewmember still onboard had similarly without knowing it spread the same malware through the e-mail he sent to his prospective new employer. They had discovered the malware and reported back to him and said they would not be interested in hiring someone who was spreading malware. The malware had also spread to the crew's welfare computer and other computers onboard when he had used a USB-stick to share the newly downloaded tv-show between the crew. Luckily it had not spread to the master's company computer onboard.

How to improve by lessons learnt

Based on the case and the keywords, you should now perform an onboard risk assessment of the incident and the factors which led to it. Bear in mind our vessel's procedures.

- You can also discuss the keywords below to determine onboard areas/topics for increased awareness:
- Not all vessels have internet access, however, onboard computers and systems still need to be updated. This might be done using CD's, USB-sticks or external hard drives. What risks are involved when updating through the Internet or by connecting external devices? How do you do it onboard your vessel?
- Smartphones and smartwatches might continuously collect your location data, without your knowledge. What are the risks of sharing a selfie or your workout-log without disabling geo-tagging? What is the company policy?
- What would you do if you discovered or someone told you that you were spreading computer malware and viruses? Do you have procedures for what to do?
- VPN, or Virtual Private Network, is a method for securing and encrypting your communications when you are using an untrusted public network. Why do most of us not use VPN when connection to an untrusted public network? Which workstations onboard have secure network connection (VPN) and which don't?
- Are there procedures in place for checking and removing unapproved or outdated software and hardware onboard? In that case what the procedures?
- Does your ship have two separate networks? Can you identify these networks? One for the crew welfare perhaps and one for ship critical and operational systems. When visitors and service people are onboard, do you allow them to connect to onboard networks? What are your procedures for such visitors?
- Using two factor authentications can reduce the risk of identity theft (username and passwords), as well as phishing via email. Do you use it?
- Is there a member of the crew responsible for cyber security training onboard your ship? Who?
- If you suspect or experience a cyber incident while onboard, do you report it? How do you report it and to who?

1 What factors contributed to the incident in the above case?

2 Risk Assessment: Could some of the factors identified be present on board your ship? What is the likelihood and severity of those factors risk factors?

3 What measures would you suggest in order to mitigate the risk that could lead to such incidents? Any additional barriers of safety that could be introduced?