Ship operators cannot afford to turn a blind eye to cyber security

Whilst investigating a cyber incident onboard a ship the USCG found that the security risk presented by the shipboard network was well known among the crew before the incident.

Published 10 July 2019

In its recent Marine Safety Alert 06-19 , the United States Coast Guard (USCG) shares its findings from an investigation into a cyber incident onboard a commercial vessel:

" *In February 2019, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network. An interagency team of cyber experts, led by the Coast Guard, responded and conducted an analysis of the vessel's network and essential control systems. The team concluded that although the malware significantly degraded the functionality of the onboard computer system, essential vessel control systems had not been impacted. Nevertheless, the interagency response found that the vessel was operating without effective cybersecurity measures in place, exposing critical vessel control systems to significant vulnerabilities.* "

Possibly the most alarming finding to come out of this investigation was that, prior to the incident, the security risk presented by the shipboard network was well known among the crew. While most crewmembers did not trust the onboard computer network enough to use it for personal matters, such as to check their bank accounts, the same network was used for official business - to update electronic charts, manage cargo data and communicate with shoreside facilities, pilots, agents, and port state authorities.

Recommendations

In light of the findings from the investigation of the cyber incident, the USCG strongly recommends ship operators to implement the following basic measures to improve their cyber security:

• segment shipboard networks into "sub-networks" to prevent unauthorized access to essential systems and equipment;
• eliminate the use of generic log-in credentials for multiple personnel by creating unique, password or ID-card protected, network profiles for each employee;
• grant a limited set of privileges to each user, i.e. limit network access rights for users to the bare minimum permissions they need to perform their work;
• establish clear procedures for the use of external media, such as USB sticks and other devices used to transfer data via USB drives;
• install basic antivirus software; and
• establish a software patch/update management policy. Vulnerabilities impacting operating systems and applications are constantly changing and timely updates is one of the most important steps you can take to protect your computer systems from cyber criminals.

As the USCG so wisely put it: " *with engines that are controlled by mouse clicks, and growing reliance on electronic charting and navigation systems, protecting these systems with proper cyber security measures is as essential as controlling physical access to the ship or performing routine maintenance on traditional machinery.* "

Additional recommendations are also available in our insight " It is time to strengthen your onboard cyber security procedures " of 12 December 2018.

Gard's safety awareness campaign on cyber security

While the IMO has given shipowners and operators until 2021 to incorporate cyber risk into ships' safety management systems, cyber criminals are already at work. Data is an asset and protecting it requires a good balance between confidentiality, integrity, and availability. Cyber security depends not only on how shipboard systems and processes are designed but also on how they are used - the human factor.

It is therefore important that seafarers are given proper training to help them identify and report cyber incidents. Based on our analysis of cases involving cyber security, Gard and DNV GL have produced a loss prevention awareness video and a presentation with some recommendations for how the maritime industry can address the issue. The material is not intended to suggest any industry changes or rule changes, but rather changes in the way people behave and act.