Maritime Ports Pushed to Up Cyber Security

September 17, 2018

By Captain Andrew Kinsey, Senior Marine

The maritime industry has traditionally been considered a safe haven for cyber security due to its physical isolation from the internet. However, with the advent of autonomous vessels, the internet of things, the ubiquity of smartphones and other mobile electronics, and the increased dependence on information technology, ports are becoming more vulnerable to cyber threats. The Port of New York/Newark is a case in point. In July, it fell victim to a ransomware attack that shut down its operations for several days, costing Maersk around $300 million.

There have been several cyber incidents of note impacting U.S. and other ports in the last two years: a critical port system in the U.K. was affected by a potential cyber attack in 2017; the Port of Panama was hit by a ransomware attack in 2018; and the Port of Rotterdam reported a cyber intrusion attempt in 2018. The financial and operational losses sustained by these incidents underscore the need for ports to enhance their cyber security defenses.

A weak spot at any point in the supply chain digital network could be all a bad guy needs to infiltrate the port systems. In the Port of New York/Newark attack, a single person fell for a phishing scam that resulted in the spreading of ransomware.

To combat this threat, ports and their stakeholders need to embrace a culture of cyber security awareness and training. Ignorance is no longer an option for the port community. "If something happened today and you go into a court and you agents, requesting that she wire a large sum of money to a vendor for some service. Fortunately, the agent thought the that appeared to come from one of the company's bigger customers, claiming it needed to see an invoice. Just one free to rifle through files looking for financial data, competitive information or the email of key company executives.

"All it takes is one person who has not been trained to not click on a link, and that's it, [a bad guy] is now in," says a weak spot at any point in the supply chain digital network could be all a bad guy needs to infiltrate the port systems. One Pinpoint

It's much, much more complicated on the cyber side of the physical security – it's the classic physically secure etc. As Chris Mason, Rajant Corp.'s director of sales for USA, says, "The cyber threat is constantly evolving, and ports must stay vigilant to ensure they are prepared for any threat."

A collaborative approach is key to building resilience. The American Maritime Security Association (AMSC) is leading the way in this regard, providing a forum for government, law enforcement, the Coast Guard and industry stakeholders to collaborate on cyber security challenges. The AMSC is urging ports to develop breach response plans, or resilience, and to prioritize simplicity for breaching adversaries. With a focus on simplicity and mitigating their risk. They need to build backup plans designed to get their facilities and operations up and operating as fast and as painlessly as possible.

Help is on the Way

If the port communities aren't worried for their businesses (and they should be), consider that from both an economic and the country's system of ports.

One of the nation's most critical infrastructures, the maritime port system employs more than 23 million people, encompasses more than 25,000 miles and includes 360 coastal and inland ports that account for an estimated 90% of the economy and the flow of goods and materials as is the country's system of ports.

Amidst growing concerns over the threat of cyber attacks, the Port of New York/Newark and other ports are taking steps to improve their cyber security. The Port of New York/Newark is investing in technology to detect and mitigate cyber threats. In addition to the ransomware attack, the Port of New York/Newark has experienced a number of incidents in recent years, including a cyber intrusion attempt in 2018.

The Port of New York/Newark is not alone in its efforts to improve cybersecurity. The American Maritime Security Association (AMSC) is leading the way in this regard, providing a forum for government, law enforcement, the Coast Guard and industry stakeholders to collaborate on cyber security challenges. The AMSC is urging ports to develop breach response plans, or resilience, and to prioritize simplicity for breaching adversaries.

The Port of New York/Newark is not alone in its efforts to improve cybersecurity. The American Maritime Security Association (AMSC) is leading the way in this regard, providing a forum for government, law enforcement, the Coast Guard and industry stakeholders to collaborate on cyber security challenges. The AMSC is urging ports to develop breach response plans, or resilience, and to prioritize simplicity for breaching adversaries.

There is also a growing emphasis on training and awareness. Ports need to ensure that all employees, from IT staff to physical security personnel, are trained to recognize and respond to cyber threats. The Port of New York/Newark, for example, is offering training to all employees on how to identify and respond to cyber attacks.

Another key to improving cybersecurity is to ensure that ports are using the latest technology. The Port of New York/Newark is investing in a number of new technologies, including intrusion detection systems and firewalls, to protect its networks from cyber attacks.

In conclusion, ports must take a comprehensive approach to cyber security. They need to prioritize simplicity, develop breach response plans, and ensure that all employees are trained to recognize and respond to cyber threats. With the right strategies in place, ports can protect their systems from cyber attacks and ensure the continued flow of goods and materials.