For insurance and enquiries please dial +372 8225 9134 or
send an email to: info@continentalpandi.com
For claims and legal advice please send an email to: claims@continentalpandi.com
For emergency please dial +372 5490 5053 or
send an email to: emergency@continentalpandi.com

Date: 21 July 2020

Maritime Cyber Attacks Increase 900%

Cyber-attacks on the maritime industry's operational technology (OT) systems have increased by 900% over the last three years with the number of reported incidents set to reach record volumes by year end.

Addressing port and terminal operators during an online forum, Robert Rizika, Naval Dome's Boston-based Head of North American Operations, explained that in 2017 there were 50 significant OT hacks reported, increasing to 120 in 2018 and more than 310 last year. He said this year is looking like it will end with more than 500 major cyber security breaches, with substantially more going unreported.

Speaking during the 2020 Port Security Seminar & Expo, a week-long virtual conference organised by the American Association of Port Authorities, Rizika said that since NotPetya – the virus that resulted in a $300 million loss for Maersk – "attacks are increasing at an alarming rate".

Recalling recent attacks, he told delegates that in 2018 the first ports were affected, with Barcelona, then San Diego falling under attack. Australian shipbuilder Austal was hit and the attack on COSCO took down half of the shipowner's U.S. network. He said this year a U.S.-based gas pipeline operator and shipping company MSC have been hit by malware, of which the latter incident shut down the shipowner's Geneva HQ for five days. A U.S.-based cargo facility's operating systems were infected with the Ryuk ransomware, and last month the OT systems at Iran's Shahid Rajee port were hacked, restricting all infrastructure movements, creating a massive backlog. Reports of this attack have gone some way in raising public awareness of the potential wider impact of cyber threats on ports around the world. Intelligence from Iran, along with digital satellite imagery, showed the Iranian port in a state of flux for several days. Dozens of cargo ships and oil tankers waiting to offload, while long queues of trucks formed at the entrance to the port stretching for miles, according to Naval Dome.

The Continental Steamship Owners Mutual Protecting & Indemnity Association Ltd
Trust Company Complex, Ajeltake Road, Ajeltake Island, Majuro, Marshall Islands

Emphasizing the economic impact and ripple effect of a cyber-attack on port infrastructures, Rizika revealed that a report published by Lloyd's of London indicated that if 15 Asian ports were hacked financial losses would be more than $110 billion, a significant amount of which would not be recovered through insurance policies, as OT system hacks are not covered. Going on to explain which parts of the OT system – the network connecting RTGs, STS cranes, traffic control and vessel berthing systems, cargo handling and safety and security systems, etc., – are under threat, Rizika said all of them.

"Unlike the IT infrastructure, there is no "dashboard" for the OT network allowing operators to see the health of all connected systems. Operators rarely know if an attack has taken place, invariably writing up any anomaly as a system error, system failure, or requiring restart.

"They don't know how to describe something unfamiliar to them. Systems are being attacked but they are not logged as such and, subsequently, the IT network gets infected," Rizika explained.

"What is interesting is that many operators believe they have this protected with traditional cyber security, but the fire walls and software protecting the IT side, do not protect individual systems on the OT network," he said.

An example would be the installation of an antivirus system on a vessel bridge navigation system (ECDIS) or, alternatively, a positioning system in a floating rig dynamic positioning (DP), or on one of the dock cranes on the pier side of the port.

"The antivirus system would very quickly turn out to be non-essential, impairing and inhibiting system performance. Antivirus systems are simply irrelevant in places where the attacker is anonymous and discreet," he said.

"Operational networks, in contrast to information networks, are measured by their performance level. Their operation cannot be disconnected and stopped. An emergency state in these systems can usually only be identified following a strike and they will be irreparable and irreversible."

Where OT networks are thought to be protected, Rizika said they are often inadequate and based on industrial computerized system, operating in a permanent state of disconnection from the network or, alternatively, connected to port systems and the equipment manufacturer's offices overseas via RF radio communication (wi-fi) or a cellular network (via SIM).

"Hackers can access the cranes, they can access the storage systems, they can penetrate the core operational systems either through cellular connections, wi-fi, and USB sticks. They can penetrate these systems directly."

Rizika said that as the maritime industry moves towards greater digitalization and increases the use of networked, autonomous systems, moving more equipment and technologies online, more vulnerabilities, more loopholes, will be created.

"There will be a whole series of new cyber security openings through which people can attack if systems are not properly protected.

"If just one piece of this meticulously-managed operation goes down it will create unprecedented backlog and impact global trade, disrupting operations and infrastructure for weeks if not months, costing tens of millions of dollars in lost revenues."

Naval Dome also predicts that cyber criminals, terrorists and rogue states will at some point begin holding the environment to ransom. "One area we see becoming a major issue is cyber-induced environmental pollution. Think about it: you have all these ships in ports, hackers can easily over-ride systems and valves to initiate leaks and dump hazardous materials, ballast water, fuel oil, etc.," Rizika warned.

Offering advice on the first steps port operators need to take to protect their OT systems, he said a deep understanding of the differences between the two spaces is vital.

"There is a disconnect between IT and OT security. There is no real segregation between the networks. People can come in on the OT side and penetrate the IT side. We are actually seeing this now. Successful IT network hacks have their origins in initial penetration of the OT system."

In a prerecorded message broadcast during Naval Dome's presentation, Rear Admiral (Retd) Shiko Zana, the CEO of Ashdod Port, said, "We have become more aware of the growing cyber threat to OT systems. Naval Dome has a unique cyber defense solution capable of protecting against both internal and external cyber attack vectors. The solution provides protection for OT systems."