CYPHRE
a RigNet company

FIRST CLASS DATA PROTECTION STEERS MARITIME SYSTEMS TO A CYBERSECURITY SAFE HARBOR

The international maritime infrastructure is becoming more vulnerable due to outdated technology aboard vessels. Known software flaws exist in the web platforms vessels use to access systems for navigation, messaging, communications, and web browsing. As an example, software bugs have been reported in the commonly used AmosConnect 8 web platform.

Attacks on the platform may provide an attacker entry into a vessel's system or expose a backdoor within the platform server. This can provide access to database information including login credentials for software aboard the vessel, and provide hacker access to full system remote commands. Two of the bugs that affected the AmosConnect 8 platform can allow cybercriminals entry into vessel's systems.

Cyberattacks can cause many kinds of damage, including long term financial consequences for the company attacked. For instance, Denmark's A.P. Moller-Maersk, reported a $1.5 billion loss attributed in part to the cost of a cyberattack.

Maritime security consultants note that these vulnerabilities largely stem from the fact that software products in this sector were not originally intended to interconnect. Some vessels have reverted to even older software versions, striving to isolate modules and close connections that can be exploited, but many vessels will remain exposed indefinitely.

Ransomware and spoofing attacks are increasingly reported. According to Congresswoman Norma Torres, a 2017 cyberattack that impacted the Port of Los Angeles revealed "serious vulnerabilities in our maritime security, and we must address these weaknesses before it is too late."

Advanced Encryption Is Key to Guarding Maritime Platforms from Cyberattacks

Proper diligence in tackling maritime platform security goes hand-in-hand with adopting powerful, proven data and communication cybersecurity solutions to provide the strongest defense against cyber threats. Cyphre's hardware driven, encryption-based full security solution protects data in-transit and at-rest. This uniquely powerful protection stretches across enterprise infrastructure, the Internet of Things, and private or hybrid clouds.

Cyphre's comprehensive solution is built on a robust data and network encryption foundation that secures maritime information behind firewalls and during transfer over private intranets or the public Internet. While encryption provides the highest level of security for data at-rest or in-transit, the way encryption is achieved matters vitally. Plaintext encryption keys held resident in the server's main memory are a well-known vulnerability, presenting a major opportunity for hackers to exploit.

Cyphre's uniquely powerful hardware-based encryption (called BlackTIE®) adds a crucial layer of protection, providing deeper and stronger data security than conventional methods can. In Cyphre solutions, encryption keys are stored in a hardware layer and are never exposed. Even if an attack enables root access into the server, the keys are protected and remain isolated from the attacker.

> In 2017, Denmark's A.P. Moller-Maersk, reported a $1.5 billion loss in part due to the cost of a cyberattack.

Securing the Industrial Internet of Things

Industrial IoT (IIoT) devices have become increasingly utilized in maritime operations to monitor: power plant performance, pumps, valves, and actuators, stability control mechanisms, as well as container tracking devices that follow the progress of goods en route to the port. These IIoT devices generate significant amounts of data that is often stored on the local network and then transmitted over satellite to a teleport or via cellular to the service provider network. Standard data encryption employed by these networks may be sufficient for consumer traffic, but is inadequate protection against modern hacking techniques used by those who want to disrupt the flow of goods or illegally access a vessel's systems. CyphreLink provides a hardware-encrypted connection for IoT data transmitted across these networks, which is highly resistant to man-in-the-middle (MITM) attacks and renders any hijacked data useless.

Looking to the Future of Autonomous Vessels

In the not-so-distant future, there may be crewless vessels operating autonomously across the world's oceans. While that may be far off, visionary shipbuilders are looking forward to a time when crews are no longer needed. In these instances, crews would be located in a centralized location where they'd be able to monitor and control vessels remotely. A vast amount of data would be generated and transmitted to the remote crew in order to maintain real-time control of the vessel. The loss of connectivity due to cyberattack may result in loss of the vessel and the goods on-board. CyphreLink can be employed to ensure protection of that data and control systems themselves, ensuring that hackers would neither be able to access the data nor inject harmful code that could hijack the vessel's operating software.

Cyphre's BlackTIE® Technology Is the Key

CyphreLink is powered by BlackTIE® Technology that extends unassailable protection for data, keys, and certificates from any end-point and across any access network. Hardware-based encryption technology leverages a specialized chipset with a dedicated security engine to offload cryptographic operations outside of host CPU and system memory - two of the most common entry points for cyber criminals. Key management controls offer total and exclusive control of the generation, exchange, storage, use, destruction, and replacement of encryption keys.

About Cyphre

Headquartered in Austin, Texas, Cyphre cloud encryption technology provides the highest level of security for cloud data. Period. Product offerings include Encrypted Cloud Storage and Enterprise Collaboration services, Secure IoT Integration and the Enterprise Cloud Encryption Gateway.

www.cyphre.com @getcyphre Cyphre /getcyphre

Copyright © 2018 Cyphre