CYBER DEFENSE MAGAZINE

eMAGAZINE

FEBRUARY 2025

In This Edition

MORE INSIDE!

Establishing a Cybersecure Maritime Ecosystem

By Sandro Delucia, Product Director, Speedcast

Cyber-attacks happen across all sectors and industries every day. In fact, they are a growth industry expanding 400-500% in the past five years alone. When these attackers succeed, the results can be critical and costly to businesses. A network breach can quickly shut down operations, resulting in millions of dollars in lost revenue and repair work. In 2023, the average cost of a successful cyber-attack was a hefty $4.45 million and total global costs per year are estimated to reach an astonishing $15.63 trillion by 2029.

Anything from a cargo ship to an oil rig can find itself the focal point of a cyber-attack, because hackers will leave no stone unturned in their quest to access a network. Shipping and maritime assets and operations are valuable targets not only because of the value of the cargo onboard, but because of their critical position within an overall supply chain.

The vulnerabilities in your networks

After years of growing cyber-attacks, most businesses have become adept at protecting ‘the front door’ of their networks – but all too often, the remote sites used in maritime and other operations are overlooked. For many businesses, these sites represent the Achillies’ heel in their overall security make-up. Currently, 24% of business security professionals report concerns about access to their sensitive data through remote sites.

By compromising remote sites, attackers can tunnel straight into the heart of a company’s network and gain access to a gold mine of potentially sensitive data. Few remote sites will have IT staff on the premises, which means they are completely dependent on the cybersecurity processes put in place by the wider business.

The critical role of endpoint security

Protecting these remote sites requires *endpoint security*. The endpoints are the laptops, mobile phones and other devices where network flows end. As companies increasingly interconnect their operations, the number of endpoints multiplies.

Protecting these devices is critical because they represent a back door with authorization to access the organization’s most sensitive data. Knowledgeable hackers will attack anything from Very Small Aperture Terminals (VSAT) to Wi-Fi, mobile, or fiber connections. Good endpoint security also addresses the human factor that is the hacker’s primary target: an employee who accidentally downloads a malicious file onto a device, for example, where it can sit unnoticed as it collects private information before reporting back to an unauthorized user.

Endpoint security is a key part of what cybersecurity experts call ‘defence in depth.’ It is the opposite of “set it and forget it,” where businesses hope a single service will ensure all the necessary protections. It involves real-time protective monitoring and threat mitigation as well as centralised, near-time reporting.

Cybersecurity as a service

The challenge for businesses is to understand which solutions will meet their needs. It is a challenge made more difficult by the constant influx of security products into an already flush market. With so many options, businesses run the risk of selecting a flashy product that doesn’t cover all their vulnerabilities through a procurement process that can be both difficult and costly.

The best-of-breed solution today is to use sector-specific solutions that offer cybersecurity as a service. In the maritime sector, for example, we’re now seeing smart network management platforms on the market, such as Speedcast SIGMA, which incorporates secure, next-generation firewalls and security policies, while giving users total oversight to what each user has access. These solutions empower businesses with a cost-effective solution which can be used to establish and maintain strong security positioning, even though its main function is to provide seamless, reliable connectivity for their networks.

Designed specifically for remote sites, smart management solutions are enabling operators to ensure the safety and security of their workforce and data flows without the need for stand-alone, cybersecurity-focused products. An industry-leading application like Cydome, for example, can be incorporated into the connectivity management system to enable real-time detection and protection, alongside managed security operations center (SOC) services. These applications run both onboard and at a fleet's headquarters, or in customer-managed virtual machines. The best provides a single dashboard that generates risk scores for each vessel and risk and compliance scores for the fleet. They can also drill down to specific vessel alerts, events, and informational and operational technology (IT/OT) assets.

When applied to smart management platforms, these applications offer that critical defence in depth, including real-time, fleet-wide monitoring; AI-based threat detection, continuous vulnerability scanning, and the latest security information and event management (SIEM) technologies for incident management.

Complying with regulatory requirements

Cybersecurity as a service is also an effective answer to the rise of cybersecurity requirements across the globe. Management teams, insurers, and regulatory bodies are now considering cyber threats with increased seriousness. This has led organizations such as the International Association of Classification Societies (IACS) to launch new and revised regulations, with the aim of tackling cyber-attacks across the shipping and maritime industries.

Take IACS UR 256/257. As of July 2024, these revised regulations require all newly constructed ships, commercial ships of more than 500 gross tonnage, passenger vessels carrying more than 12 people, self-propelled units and drilling rigs working offshore to adhere to new, stringent regulations.

UR E26 focuses on providing a minimum set of requirements for the cyber resilience of the ships themselves. It means vessel inventories must be updated and administered in detail, alongside an analysis of access control across systems. Alarms and testing must also be evident across vessels in order to adhere to the new requirements, representing a significant security enhancement of onboard systems.

IACS UR E27 specifically covers 41 security capabilities relating to onboard device systems and equipment. Some of the main security features that must be implemented include multi-factor authentication, cryptographic algorithms and regular audits. This will ensure a strong line of defence against potential cyber-attacks.

Non-compliance with any of the proceedings outlined by UR E26/27 will result in significant financial and legal penalties, as enforced by another recently revised European Union regulation, the NIS-2 Directive. Companies will be subject to fines up to a maximum of €10 million or 2% of their global annual revenue if deemed to be neglecting these regulations.

Greater vigilance, reduced vulnerability

As harsh as the regulations and penalties may appear, their aim is to create a state-of-the-art cybersecure maritime ecosystem. Decision makers must now find the best way to ensure compliance while balancing the investment cost and benefit.

The maritime industry has been considered a soft target for hackers, where remote devices were weakly defended from external attack and offered an open road into the enterprise network. Cyber risks once seemed limitless, daunting, and without a cure. But in reality, they are much like the risks of every voyage: manageable, as long as vigilance never ceases.

About the Author

Sandro Delucia is a Product Director at Speedcast. He has over twenty years of international experience in Telco and Satellite Communications and has worked extensively in the sphere of Product Management on complex MSS and VSAT projects and solutions. He is actively engaged in driving Speedcast’s standard, and bespoke solutions with an emphasis on driving intelligent edge, operational and cloud solutions, and is continuously seeking innovative ways to enhance customer experience and value derived from customized IT and connectivity solutions.

Sandro can be reached on LinkedIn at https://www.linkedin.com/in/sandro-delucia-b3566a1/ and at our company website https://www.speedcast.com/