INMARSAT takes mature approach to maritime cyber security

The threat ships face from cyberattack demands a response to technical, operational, training and insurance needs. Inmarsat is separating fact from fiction as it prepares to launch the industry’s first fully managed unified threat management service, says Senior Vice President Safety and Security Peter Broadhurst.

The Dyn cyber security breach of October 21, 2016 saw multiple denial-of-service attacks target the Domain Name System provider which, it turns out, supports Internet platforms across Europe and North America. Victims included Twitter, Paypal, Spotify, CNN, and the New York Times, as Mirai malware triggered lookup requests from tens of millions of IP addresses. Printers, cameras, home gateways and even baby monitors conspired to load attacks in 1.2 terabits per second waves.

The maritime sector is far from immune to the hacking threat. In August 2016, French naval contractor DCNS fell victim to a hack that left The Australian newspaper holding 22,000 documents detailing the design of a submarine under construction for the Indian Navy, including combat

The Short Read

- Cyber security breaches on the rise
- Maritime sector is prone to attacks
- New awareness campaign gains support
- Inmarsat developing solutions

IMPA.net
Marine Trader

capability. In the same month, US ports reported attacks using an SQL injection flaw to the Web-based component of widely used Navis maritime transportation logistics software suite.

Then, in October, 2016, Hewlett Packard disclosed that a hack of United States Navy records from a sailor’s laptop within its Enterprise Services agreements had given access to personal records of more than 134,000 sailors.

Many in the maritime sector nonetheless still assess the probability of premeditated cyberattacks on shipping as low. This must be one explanation why a recent Coventry University study supported by the CSO Alliance (Company Security Officer) found 100% of participating shipowners saying their crews were given no training in cyber security at all.

As land-based users know, however, ‘freedom’ to roam the web is just as open to fraudsters as it is to legitimate users. This year has also seen the launch of the ‘Be Cyber Aware at Sea’ campaign by UK-based maritime cyber security specialist JWC International, which we at Inmarsat are actively supporting and has attracted support from The Standard Club, North P & I Club, and insurance broker, Integro.

Yves Vandenborn, The Standard Club Director of Loss Prevention, says: “This emerging threat is very real and current. Technology on ships continues to advance and so do the challenges that arise as a result. Educating crew and spreading awareness is the first step in fighting

“The maritime sector is far from immune to the hacking threat”

Source anything, anywhere...
GET THE CODE

The IMPA Marine Stores Guide 6th edition DATA LICENCE has arrived!

The Marine Stores Guide is the world’s leading reference code within the maritime industry. The MSG Data licence provides a universal coding system to facilitate communication between crew, owner and supplier, making the specification and supply of goods simple quick and effective.

With the latest and most complete version of the data now available, there’s no better time than now to start using the unique six digit code in your IT system.

The data features more than 43,000 products provided by suppliers and manufacturers from around the world. Regular updates are included as part of the licence.

www.marinestoresguide.com | +44 (0) 1206 798 900
cybercrime at sea”.

The sentiments and the ‘Be Aware’ campaign are warmly welcomed by Peter Broadhurst, Inmarsat Maritime Senior Vice President Safety and Security. Inmarsat recently ring-fenced Maritime Security as a dedicated area of expertise within Safety Services, with a team of nine cyber specialists.

Inmarsat is developing an end-to-end cyber security solution, which “includes a technical answer to report and prevent attacks or malware on a ship, but also offers a programme of awareness, risk assessments and the training that drives best practice procedures”, Broadhurst says. Part of the cohesive approach sees Inmarsat seeking to include its cyber security capabilities in a scheme to upgrade of its network and infrastructure accreditation in line with ISO27001.

In a world where half of online traffic is automated and an entire black market supplies hackers with tools to breach corporate security, Broadhurst is nonetheless keen to keep shipping’s cyber threat in proportion. “I think there are cyber companies out there now who have made their mark with the financial institutions and are looking to other verticals; superficially, they can make an impression by predicting doom and gloom on the cyber threat to shipping,” he says.

Although ships can be carrying high value cargoes, many individual vessels do not have large amounts of valuable data onboard; their attractions for hackers is that they offer a way in to a company’s corporate system. “The reality is likely to be that the systems are under attack because they are identified as IP addresses by hackers who are looking for any weaknesses to see what they can get their hands on, and not because they are ships or shipboard systems” says Broadhurst.

Inmarsat is working within a strategic alliance with Singtel to utilise capability available through the Singaporean telecoms company’s Trustwave subsidiary. Shipboard tests of a maritime UTM (Unified Threat Management) system from Inmarsat are currently underway and the full launch is envisaged later in 2017. The Inmarsat solution will be embedded in all Fleet Xpress hardware going forward, as an option which can be switched on or off by the operator as required. In the future, the same capability will be extended to FleetBroadband, Broadhurst says.

The technology will be supported through a network of already established security operations centres, Broadhurst continues. “Owners will be able to get a view of what is going on at both the ship and the fleet level, and track causes behind any security compromises, whether they are due to attacks or to the presence of malware on board. We also see the system’s use as the basis for improving training and achieving the best practice that block threats coming from malware.”