www.worldcommercereview.com

Innovative cybersecurity

Adamson Middleton's Marine Technology Specialists present Mobile Device Management & Live System Monitoring to prepare the maritime industry for future cybersecurity threats

In June 2017, a global cyberattack, known as Petya, targeted various international industries, but the Trojan horse virus also heavily infected the maritime industry. Cybercrime prevention is in increasing demand as cybersecurity threats continue to develop with more advanced and problematic variations of malware.

What began as a harmless looking software update for accountancy programmes, essential for companies working with the Ukrainian Government, became one of the most notable global cyberattacks in history. The attack utilised payloads that infected the computers' Master Boot Record (MBR), overriding the Windows bootloader, and consequently triggering a reboot. This allowed the attackers full access to the computer and as reports of similar infections spread across mainland Europe, thousands of computers and networks were being controlled by the attackers, as users and companies were held to ransom for large sums of bitcoin to end the attack.

As a consequence, multinational companies were affected; including British advertising and law firms, French construction and retail companies, American hospital operators, and a Russian oil company. It also caused the radiation monitoring system at Chernobyl to fail. The attack marked a collaboration of international governments to combat cyberattacks, yet Petya's notable differences marked it as next generation in malware technology.

Unsurprisingly, the advancement in malware technology prompted the development of protective systems around the globe, but while governments focused on the financial industry, the yachting and maritime industry were left to defend themselves.

More than a year on from Petya, the maritime industry is still in dire need of advanced security protocols to brace against the force of developing cybersecurity threats. Most users think it won't happen to them, and it's something that only happens to other people; or that their free antivirus software is enough to protect them, but this is simply not true. With more and more people being connected on multiple devices and across multiple locations, cybersecurity has never been more important.

At Adamson Middleton, the team found that their clients were looking for a complete package from one location including their luxury assets (including aviation, automotive, real estate, art and collectables), yacht management and crew recruitment but also for security and support online and on-board.

> *Cybersecurity has become a growing issue for business and leisure environments with multiple devices, and the yachting industry has also felt the brunt of vulnerable security systems which threaten the entire vessel*

As a result, in the lead up to the Monaco Yacht Show 2018, they introduced their new brand, Adamson Middleton Marine Technology (AM Marine Technology), providing global internet connectivity, entertainment packages and security solutions for marine clients by teaming with some of the industry leaders.

The technical specialists at AM Marine Technology have highlighted the need for consolidated connectivity solutions for the yachting industry, providing internet services which provide access to the best entertainment services and secure connections to the internet; a security gateway (including monitoring, management and traffic routing), and remote support from their team of experts. They also provide consultancy for both new and existing vessels ensuring that each yacht receives the best connectivity solutions and are prepared to weather the storm against the strongest threats.

The Internet of Things (IoT) has offered the availability of interconnected items, but better-connected devices also present difficulties in protecting the entire system. With a growing network, IoT devices are no longer isolated. They have moved from the workplace, into our homes, and will undoubtedly have a lasting impact on our lives. Using social media, spam emails and Trojan viruses, modern hackers can gain access to your devices, collecting personal and confidential information.

They no longer need to specifically target devices, primarily because interconnected items present the availability of one vulnerable device, which inadvertently infects the other items. The security issues IoT has raised have not gone unnoticed in the yachting and maritime industry, and with pre-existing problems, vulnerable devices on-board present new and arising difficulties in protecting private yachts from a total security breach.

Cyber criminals attack without discrimination of person or device with a blanketing approach. Steve Debnam, Technical Solutions Expert at AM Marine Technology, said *"Take a moment to think about the saved passwords and* *personal data you have stored on your mobiles, tablets, laptops and computers. It will not take long for you to unveil the devastating pattern that modern hackers are experts at discovering! Now, ask yourself, what security do I have that fully protects all of my devices?"*

Hackers look for easy access to devices lacking security systems, and the average user is more likely to breach your security systems accidently, rather than by direct breach of security via firewalls and internet services. There are two systems which perfectly secure backdoor security and work alongside Antivirus and Firewalls; Mobile Device Management and Live System Monitoring. According to AM Marine Technology's leading experts, these are now recognised as essential aspects for any interconnected environment, but especially within the yachting industry.

Recent international conferences surrounding the discussion of IoT devices have highlighted fundamental flaws in IoT architectures, meaning interconnected devices, such as mobiles, tablets and laptops, connected to a yacht's network have initial flaws which leave the bundle of devices primarily unprotected and weak.

Mobile Device Management, commonly known as MDM, is a solution that secures mobile devices, preventing them from attacks targeting the weaker items within the network, while still allowing full control of the internet connectivity to the owner, captain and management crew. MDM is a security software used to monitor, manage and secure mobile devices that can be deployed across various networks. Amongst numerous features, MDM secures emails, documents, browsers and app catalogues, ensuring all items are contained.

This has proved particularly useful for environments where large amounts of data are stored. This could be both personal and professional information. The yachting industry is fortunate to have internet solutions granting each vessel with its own network and servers, yet this makes the yachting industry weaker as individualised networks could potentially come under attack. Solutions such as MDM ensure security threats are taken into consideration and avoided.

Debnam added *"Any device used by the crew or guests while on board has the potential to be a threat, and the moment any device is brought on-board, or there is potential for a device to connect to your network, they can breach the security of the vessel.*

"MDM with AM Marine Technology, allows yacht owners and captains to set their own limits and decide which devices may access their network. Meanwhile the managerial aspects of maintaining the system, on a daily basis, is left to the Technical Specialists. Data is a difficult and tiresome topic to grasp but the threat on incoming devices from crew and guests is not, so the availability of continuous remote support and device management will prove essential in protecting vessels from cyber threats."

Similar to MDM, Live System Monitoring is one of two solutions which will prove essential for the future of internet security in the yachting industry. Anyone using your network can become a potential security breach, and it is quite common for information to be lost or stolen via backdoor access by remote login or information theft.

These monitoring systems are used to keep track of system resources and network usage on-board vessels. They enable yacht owners, captains, crews and guests to remain completely secure from potential cybersecurity threats whilst on-board or on land, and they prevent the intrusion of unnecessary or uninvited users that may pose a threat to the vessel's network.

"Live System Monitoring tracks every user system to fine tune monitoring at an individual level;" said Debnam, *"it prevents the possibility of disgruntled former employees having remote access or sharing files and information with unsafe sources."*

Preparing for disadvantageous situations does not ideally befall the yachting industry, yet it is paramount to the security of every vessel that possess entertainment systems, internet services, or any form of connectivity which allows you to communicate with the outside world.

Security threats are not a new issue in the yachting industry, but with hackers finding easier access by penetrating vulnerable devices which infect multiple, if not all, devices on-board, the industry is in increasing need of more advanced security solutions.

The availability of MDM and Live System Monitoring from AM Marine Technology provides a solution to an age-old problem within the yachting community. Technology has become as crucial as other aspects of the yachting world, and although this is led by the demand for more advanced and better equipped vessels, technology has also seen significant development in security measures.

Disgruntled former employees, incoming guests, and the crew manning the vessel may all carry devices which are potentially damaging, because they have the option to connect to your network, but the devices themselves may already be vulnerable and susceptible to attack. The network hosting the device does not necessarily know the device is weak but unfortunately hackers are looking for any vulnerable devices and once they connect to the yacht's network, they can upload their virus which has the potential to have devastating consequences on your vessel.

Alternatives such as Live System Monitoring offer yacht owners and captains security protocols to protect against potential infections, although there is no guarantee, as any device is harmful and there is always the possibility that any device could be weak enough for the cybercriminals to infiltrate.

There have been cases of hackers being able to infiltrate vessels and turn them off course, and other cases of documents, emails and both personal and professional data being removed or stolen. This threat only continues to grow, and as cybercriminals develop more advanced viruses, it becomes increasingly difficult to combat various forms of attacks which look and act like your everyday network.

The introduction of MDM and Live System Monitoring has enabled companies such as Adamson Middleton to protect the yachting industry from threats of this magnitude, and their endeavours with Marine Technology Technical Specialists have allowed them to provide protocols to support and protect their clients from various cybercrimes which allow their customers to enjoy the luxury lifestyle which was intended.

Cybersecurity has become a growing issue for business and leisure environments with multiple devices, and the yachting industry has also felt the brunt of vulnerable security systems which threaten the entire vessel. Security solutions, provided by AM Marine Technology, can combat the developing threats associated with the yachting industry, as well as securing all incoming devices from crew members and guests, ensuring vessels are given the correct level of protection. ■