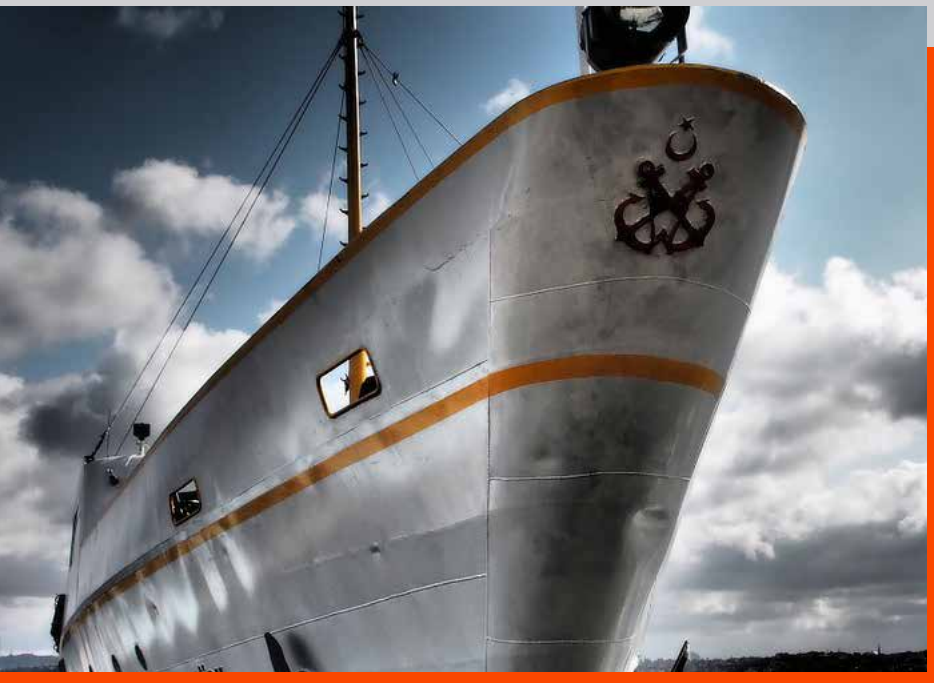
#4

MAR:2017

PHISH & SHIPS

BE CYBER AWARE AT SEA



Kindly sponsored by

CSO ALLIANCE MARITIME

BE CYBER AWARE!

Welcome to issue 4 of "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with a new industry initiative, "Be Cyber Aware At Sea".

2017 will be the year hackers innovate, according to cyber experts. It will also be the year that hackers begin to get more creative, most likely expanding their areas of operation. Meaning that shipping could come into the cross hairs.

In the past, cybersecurity was considered the realm of IT departments, but no longer. Smart companies now systematically integrate security into their systems, and adopt proactive policies.

Companies need to identify internal vulnerability to hacks and to apply preventative best practices. There is no option but to take a good hard look at what is being done, and what can be done better. Asking what can go wrong, and how vulnerabilities can be plugged.

Alas for many companies it is not always easy to understand the cybersecurity threats they face. This is especially true in shipping, and there is a black hole developing, which can mean a worrying gap between IT departments, vessels and of senior management ashore.

Within these roles there is much information, but it seems we are not asking enough questions about cyber threats and responses.

So it is time to ask the difficult questions, to look at the systems, people and the way in which data is stored and manipulated. Where are the problems? What would happen if something went wrong?

There can be no hiding, no putting the collective corporate head in the sand. This is a real and ongoing threat, so it is vital to address cyber security now. We hope the Be Cyber Aware At Sea campaign helps and makes a difference.

This latest issue of Phish & Ships has been kindly sponsored by CSO Alliance, an organisation which is mobilising the global community of CSOs to more effectively counter all aspects of maritime crime.

According to Mark Sutcliffe of CSO Alliance, "working with credible cyber sector experts and our existing maritime industry supporters we will be putting at the disposal of the shipping and port community a collaborative crime reporting tool".

This Maritime Digital Platform enables the reporting of Cyber Incidents impacting the maritime community operations at sea and on-shore.

This community tool helps drive a better understanding of the impacts, evolution of best practice, as well as developing effective prevention and responses to Cyber incidents. See their website for more details www.csoalliance.com

Cyber issues can be technical, but sometimes it is about a simple lack of common sense. Just last month an Indian Navy Spokesperson took to Twitter to give a, "rough location and approach time" as the naval vessel headed to the conflict zone in Yemen.

Responding to a supposed distress message posted on twitter from an Indian vessel stuck in Aden. Seemingly without thinking of what could go wrong, the location of the Indian Navy ship and time it would take to arrive was tweeted.

Online risks mean being cautious and acting with care. So think before you tweet or post. Who could be reading the message? What could go wrong? STOP and THINK before you post.

Be discreet when you tweet!

INSIDER THREAT RISKS

As organisations adopt more effective strategies to defeat malware, it is the belief of most cyber security experts that attackers will have to become more innovative.

They will likely shift their approach and start to use legitimate credentials and software to access systems. This means that companies need to think about physical insiders and credential theft.

There will also be a likely increase in targeting of social media and personal email bypasses to get past network defences, using email scams and bypassing company URL filters.

The most dangerous aspect is how attackers manipulate victims with enticing offers such as jobs or wealth, or even threats and access to illicit content.

The insider risks is very hard to deal with, and it will be necessary for defenders to focus on inconsistent "user behaviours", as these are the most effective way to differentiate malware and insider threats from safe and acceptable content.

Sponsored by: CSO ALLIANCE MARITIME

ARE WE READY FOR AUTONOMOUS SHIPS?

Rolls-Royce is planning to release the first of its fleet of crewless ships by 2020. The firm is working with government-backed groups across northern Europe on autonomous vessels and estimates that the move could cut sea transport costs by as much as 20%.

Major shipping firms are expected to adopt the technology in the hope it will boost profits. However, autonomous ships present challenges for insurers who have to consider the new types of risks that they will face.

Rolls-Royce, for its part, maintains that crewless ships will be both safer than existing vessels and that they will lead to the creation of more jobs on land.

The company says it is embarking on major research projects in the UK and Singapore - and that it believes the development of autonomous ships will increase demand in areas such as cybersecurity.

Indeed, there has been much concern that until issues of cyber risk are addressed, then autonomous ships will never become a mainstream reality. At the moment there are many concerns to be dealt with, and while the dream may sound attractive, it could become a nightmare if navigation or power management systems were to become infected. Learn more about autonomous ship at www.rolls-royce.com

Cyber Jargon Buster

PHYSICAL INSIDERS - These are the people within your company who have legitimate access to systems.

CREDENTIAL THEFT - Cyber criminals hunt for user and corporate credentials (usernames and passwords) and steal them for access.

"MAN-IN-THE-APP" - a proxy Trojan that infects by taking advantage of vulnerabilities to modify pages and transaction content, all invisible to both the user and host application.

EMAIL SCAMS - A simple but effective means of tricking people into revealing data - usually bank details or access credentials.

URL FILTERS - URL filtering prevent users visiting unsafe websites, viewing inappropriate content and unintentionally downloading malware.

Watch Out for Trojan Ship Attack

Shipping companies are beginning to take cyber threats seriously and one company which runs a fleet of oil and gas carriers recently identified a trojan virus which could wreak havoc. In a security advisory, Consolidated Marine Management's (CMM's) cyber security department said the "AlienSpy" remote access trojan (RAT) could be set to attack shipping.

A trojan virus is a destructive program that appears to be a benign application. The RAT could be lurking in a Java file, or even within popular office documents such as Microsoft Word and Excel, or even Adobe PDF files.

AlienSpy is the latest in a family of RATs which target victims in a bid to steal valuable data and compromise systems. These kinds of trojans, often deployed through phishing campaigns which use spoof emails and malicious files to deliver malware payloads, can be tailored to target particular industries – and so shipping could be particularly vulnerable.

This trojan is a real problem and is currently supporting infections on Windows, Linux, Mac OSX and the Android mobile operating system. Once deployed, it grants an attacker access and control over a compromised system. The malware is able to collect system information including OS version, RAM data and computer name, upload and deploy additional malware packages, capture webcam and microphone streams without consent, and remotely watch device activity. In addition, the Trojan includes a keylogger.

RATs are very common and designed to provide the attacker with complete control over the victim's system. They can be used to steal sensitive information, to spy on victims, and remotely control infected computers. The infections are typically carried out via spear phishing and social engineering attacks.

CYBER PROTECTION FOR THE ROYAL NAVY

Lt Cdr Tim Parker RN CEng CITP CISSP is a Cyber and Information Security Professional bridging the gap between technical experts and executive management.

Here he discusses the steps being taken to bring cyber protection to the Royal Navy.

A maritime platform, as this community will be well aware, is a complex thing and the provision of cyber protection is equally complex. For us, the challenge is exacerbated by the variety of platforms and systems which must be considered – there is simply no "one size fits all" solution. Equally, the problem is as much social as it is technical; both from the perspective of awareness and understanding and also that human factors are a significant contributor to the majority of incidents.

A key early lesson is that this problem is not just about Information Technology (IT) – the traditional networks and user devices, but just as much about the Operational Technology (OT) – the control systems which make our platforms function. We have to consider each and every element of IT and OT to ensure that we are mitigating the critical vulnerabilities and protecting what is truly valuable.

On a practical note, given the physical constraints on a maritime platform, we cannot just allocate some space to a Security Operations Centre (SOC) because that space generally is already taken up and we also can't just add another X personnel to the ship's company. So, we have to rely on existing personnel, who are already busy and who are unlikely to be deep specialists in cyber protection, meaning that any additional workload must be accepted and recognised as necessary.

Bringing all this together, our early approach has two main strands; user awareness and cyber protection.

The user is the first line of defence and it is essential to deliver an enduring campaign of cyber awareness training, education and messaging to ensure that our users are as fully aware as possible of the ever evolving and ever present cyber threat. It is for this reason that we are proud to support the Be Cyber Aware at Sea campaign and recognise that a common message across the seafaring community is far stronger than an internal campaign.

Our approach to cyber protection is one of layers, with the initial layer formed of a Cyber Essentials baseline to reinforce a foundation of good behaviour and good practise, much of which was already established. The benefits of using Cyber Essentials is that it is an externally validated scheme and because it is effectively a reinforcement of good system administration, it can be implemented anywhere, at any scale and by anyone who is already a trained system administrator. It is appropriate for any size of platform or unit and the principles can be applied to IT and OT.

The combination of aware users and a solid foundation of protective principles sets us on the right path and is suggested to mitigate around three quarters of the threat. Crucially, it ensures that future developments are set against a backdrop of good behaviour. The details of the upper layers sits outside the scope of this article, but suffice to say there is an element of upskilling existing personnel to provide greater on-platform protection, coupled with off-platform protection where connectivity and infrastructure allow. This will be supported by a centre of excellence to coordinate and focus our efforts and augmented by deployable teams.

Is any of this easy? No! Is it necessary? Absolutely! Are we headed in the right direction? Yes!

5 Easy Ways to Get Yourself Hacked

1. Clicking Malicious Links - beware of emails asking you to click phishy links
2. Torrents - Those free files may be tempting, be careful what you wish for
3. Popups - Dodgy websites can bring all kinds of bad things into your system
4. Scams - You have been chosen to receive a billion dollars. No you haven't - you are being scammed!
5. Drive-by Downloads - Your security settings may make you a target

Source: theMerkle.com

JOIN IN AND HAVE YOUR SAY...

To keep up with the cyber risks to your company, fleet and onboard your ships, make sure you visit our website and join the campaign to make maritime cyber security work.

www.becyberawareatsea.com

think@becyberawareatsea.com

Steven Jones, the editor of this monthly round-up of maritime cyber matters, would love to hear from you.

So please share your thoughts, views and experiences with the industry. We will analyse the current state of play in our next issue. Together we can help the industry to Be Cyber Aware at Sea.

TALKING CYBER SENSE WITH NOVAE: GPS SPOOFING

Novae
LOOKING FORWARD

TALKING CYBER SENSE: Sharif Gardner, Head of Training at Novae Group shares his thoughts on mitigating cyber threats, this time we look at GPS Spoofing and threats to navigation.

The world we live and work in is becoming "digitalised". While the new technologies are advantageous and bring efficiencies for organisations, they are also accompanied by a range of threats and the marine sector is not immune from these risks.

Today's onboard Operational Technology (OT) and Information Technology (IT) systems are beginning a journey to becoming connected like never before and the reliance on smart and interconnected systems will grow as shipping companies strive to be faster, cheaper and more efficient.

The shipping industry is heavily reliant on GPS (Global Positioning System) and there is a fear that the reliance and "digitalisation" of the industry means that the system is at risk of unauthorised interference, spoofing attacks.

Spoofing is a surreptitious attack which tricks the navigation system. A fake GPS is created that emits a counterfeit signal stronger than the real GPS signal.

If you can hijack the communication between the satellite and the system, then hackers could input incorrect coordinates into the system leading the officer of the watch to steer the vessel off course, resulting in significant financial, safety, security and business repercussions for shipping operations.

However, the likelihood of this happening in today's environment is low and the human element is one of the first lines of defence in the shipping industry.

There are primary, secondary and tertiary controls in place to mitigate this risk and these countermeasures help secure the systems.

Those operating the vessel can engage in the following to mitigate the risk: monitor the absolute and relative GPS signal strength, monitor the signal strength of each received satellite signal, monitor the satellite identification codes and number of satellite signals received, check the time intervals, check on the veracity of the received GPS signals, use the vessels gyrocompass to independently monitor the physical trajectory of the receiver. Completing these checks will identify any suspicious activity and decrease the likelihood of a successful spoofing attack.

https://www.novae.com/

GROWING FEAR OF OIL AND GAS ATTACKS

Globally, it is estimated that cyber-attacks against oil and gas infrastructure will cost oil and gas companies US$1.9 billion by 2018.

There are many reasons why the threat posed by cyber-attacks has grown recently in the energy industry. Such is the industry's overall global profile that it is clear that there might be any number of individuals or groups that would have sufficient motivation to launch a cyber-attack, if they felt that it would have a chance of success.

The problem is particularly acute when considering the areas of the world where high levels of oil and gas production and infrastructure sit side by side with political or environmental groups that are prepared to use cyber-attacks as a weapon.

The oil and gas industry is well aware of potential threats, and is rising up to tackle cyber security issues by creating joint programs and initiatives. From rogue employees, to environmental lobby groups and even government sanctioned attacks, the oil and gas industry can sometimes seem squeezed on all sides.

It is not even as if there is a straightforward solution. Experts say that technology alone is not the 'easy fix' that cyber security needs: boosting security can come only by raising awareness among personnel, which makes campaigns such as Be Cyber Aware at Sea even more important.

Lest we forget the industry has already suffered an incredible hack - back in 2012 one of the biggest oil companies in the world, Saudi Aramco was hit and hit hard. It wiped 35,000 computers in hours, and Aramco was forced to use fax machines and typewriters. In a matter of hours, Saudi Aramco's ability to supply 10 percent of the world's oil was put at risk.

This is prompting a response, and DNV GL has set up a Joint Industry Project (JIP) together with A/S Norske Shell, Statoil, Lundin, Siemens, Honeywell, ABB, Emerson, and Kongsberg Maritime, to develop the best practices in addressing cyber threats.

For those tempted to think that low oil prices means less risk, think again, and the time to act is now.

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our Supporters