#7

JUNE:2017

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

CSO ALLIANCE MARITIME

MAJOR CYBER WAKE UP CALL

Welcome to issue 7 of "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with the maritime and offshore industry initiative, "Be Cyber Aware At Sea".

The issue of cyber security has come to the fore in the media in recent weeks, prompted by the ransomware attacks on the National Health Service (NHS) in the United Kingdom.

The concerns over the effect of such a large scale attack have rumbled on, but the knock on effect has been a reassessment of the vulnerabilities in other industries, including shipping.

Amongst the various reasons that the NHS was seemingly vulnerable to attack was the fact that many hospitals and surgeries use out of date operating systems, and sometimes ones which are so old they do not even receive security updates anymore. It came to light in the media that use of old computers running Windows XP is still commonplace within the NHS, and that has made them vulnerable.

Microsoft ended support for Windows XP back in April 2014. That meant no more security updates or technical support for the Windows XP operating system. Which in turn means that anyone running XP is hugely vulnerable to viruses, malware and, as we have seen, ransomware.

The message from Microsoft has been extremely clear – they have said that it is very important that customers and partners migrate to a modern operating system, their own variant currently being Windows 10. It is also important to note that the company has gone on to stress the importance of such a move. They have stated, "Customers moving to a modern operating system will benefit from dramatically enhanced security". This is of particular relevance to shipping.

There are far too many vessels using computers which still operate with Microsoft XP. Incredible as it may seem, hugely costly vessels are being left vulnerable because of a lack of modest investment to use the latest software. This is a massive concern, and there are serious security implications.

It is imperative that shipowners, operators and managers are aware of the problems that outmoded and out of date software can cause. It is then also important to act and do something about it. The old proverb goes that you shouldn't "spoil the ship for a ha'porth of tar", and today that premise still applies.

Don't put the lives of seafarers at risk, don't make ships vulnerable, or put cargo at risk, for the sake of investment in the right IT tools to do the job. So, Be Cyber Aware At Sea, and do the right thing to protect shipping from the many cyber risks facing it.

Human Hackers at the Gangway…

The issue of human hackers at the gangway is a major concern, as we see social engineering at sea. Jenny Radcliffe a.k.a "The People Hacker" is a specialist in the psychology of social engineering attacks and defending against them. A life long social engineer herself, she specialises in helping organisations spread awareness of "human hacking" methodologies and protecting their staff and companies from malicious social engineers."

Social Engineering is a relatively low risk method of attacking an organization with a view to breaching it's security and accessing data, information or else that which is considered of worth. A non-technical "hack", it relies on exploiting human vulnerabilities and manipulating behaviour to open up a system, organization or company to being breached.

Whether by forming bogus relationships online or in person, or from profiling a target through details obtained via social media, human hackers find the "in" via manipulating human beings. In terms of security, this human "weak link" has always been a problem to be addressed, even if the terminology used to describe it, and the tools used to facilitate it, have changed.

Recall the "loose lips sink ships" style awareness campaigns of WW2, proving that years before "cyber" was a term in popular use, the idea of keeping information private in order to protect ourselves has long been a concern. It is a message that needs to be continuously reiterated at sea and beyond, as in the modern world the sharing and misuse of information is easier and more prevalent than ever before.

Information concerning logistics, movements and people, however irrelevant or loosely connected it might seem, is dangerous because it helps build up a picture for attackers. Details such as which football team someone supports, how they spend their free time, hobbies, passions and family, can all be used as leverage to build rapport, persuade, or coerce individuals to unknowingly or through duress, assist an attack.

In this digital age the gangway might be physical, psychological or digital but it still needs protecting, the methods might have changed, but the goal of the enemy is still the same, as is our defence against human hackers. Discretion and caution is still advisable, especially online! Loose lips, (and clicks) STILL sink ships!

UK MARITIME & COASTGUARD AGENCY APPROVE THE GCHQ MARITIME CYBER SECURITY AWARENESS COURSE!

The one hour online e-learning course which has been developed by JWC International, a leading maritime education provider has now been approved by the UK flag, the Maritime and Coastguard Agency (MCA). The course which is available through a web based maritime cyber platform, provides news updates, posters, videos and cyber risk assessment templates for ship owners and managers is the first of its kind.

The platform has been developed in partnership with Navarino, the maritime industry's most advanced communications and connectivity company. We spoke to Commodore Geoffrey Billson RN (Retd) from JWC International and Ray Brough, Managing Director at Navarino about this latest development.

Commodore Billson highlighted the importance of accreditation: "This MCSA course has really set the bar in terms of awareness training for seafarers worldwide. With GCHQ approval and UK flag approval acting as two kite marks of excellence and quality assurance for ship owners and crews. Previously the course was a classroom based one day course but after feedback from industry it was clear a much shorter, less technical and basic awareness solution was exactly what was required. This has made it much more accessible for seafarers worldwide and comes with immediate GCHQ and MCA certified training on successful completion.

Ray Brough from Navarino added, "Cyber Security is an emerging threat to the marine industry and one that we have a duty to help our clients understand and become more aware of, in an increasingly connected world. Navarino are delighted to have partnered with JWC International to bring the the first GCHQ and MCA approved course to our customers, this is a significant development for industry"

The course content includes:

- Malware Awareness
- Phishing & Social Engineering
- Passwords
- The 'Insider Threat'
- Securing Mobile Devices & Removable Media
- Responsible Web Surfing
- 10 Essential Steps to Maritime Cyber Security
- Case Studies

If you would like more details on the MCA course, please visit: www.maritimecybertraining.online

TACKLING SUPERYACHT CYBER WOES

The issue of superyacht cyber security has been the subject of high profile review of late. Just recently even The Guardian newspaper was caught up in a frenzy of excitement, as it was warned that hackers could access superyacht systems and sail yachts, and their "super rich owner – off into the sunset".

All pretty sensational stuff and while it can be all too easy to fall for the hyperbole, the fact remains that the threats and vulnerabilities are all too sadly real. With just a laptop hackers are able to control a vessel's satellite communications, and navigation. Hackers can read, delete or even edit emails, and can even send the yacht off course. Then they just wipe all the data and erase the evidence.

Journalists have been stressing the "ease" with which "ocean-going oligarchs or other billionaires can be hijacked on the high seas". Indeed, criminal gangs could exploit lax data security on superyachts to do whatever they wish. From stealing owners' financial information, through to private photos – and even the yacht itself. Such tales are truly terrifying, and very, very real. The Guardian article reported on the recent Superyacht Investor London conference, where cyber was a hot topic.

The problem exists, and the fallout is being felt. It was reported that one billionaire had more than £100,000 stolen when criminals hacked his bank account while onboard, while other high profile, high net worth individuals have reportedly been blackmailed with compromising photos, while some have been forced to pay a ransom to unlock the vessel's navigation systems.

It was stressed that yachts are often vulnerable due to less-secured Wi-Fi networks. There is also the fact that very often they tend to have strong signals. So they can easily be spotted and accessed, as all too often the networks extends quite far from the actual yacht.

Data hacks leading to blackmail and ransom demands had become more common in the past 18 months and so the problems is growing. There is also a parallel problems for superyachts, and that is crew posting to social media. So there are a number of issues which need to be addressed, and there can be no avoiding the fact that superyacht cyber security is a very important consideration indeed.

Digital Ship

THE MARITIME CIO FORUM
Tokyo - 30 August 2017

Shipping is waking up to a new era, where digitalisation is creating increased opportunity for development and innovation. With this in mind, Digital Ship is excited to be heading back to Japan to hold the next in our series of highly respected Maritime CIO Forums, where the focus will be on how to drive these opportunities, and how to address the challenges and questions these advances in technology are posing to our industry.

Through three key sessions, we will ask how the industry is responding to change and investigate what technology and digital transformation can do for us.

Session 1: The Maritime Satcom Summit

Investigating the evolution of maritime mobility and connectivity: The ever-growing use of onboard applications and increased data flows – such as those used for maritime safety and protection, vessel tracking and performance analysis – means that the shipping sector requires ever more reliable data communications, even in remote locations.

This opening session of the day will look at how innovation and evolution in maritime connectivity is changing the maritime landscape by improving operational agility, enhancing efficiency, creating a safer, more secure environment for passengers and crew alike, and above all reducing costs for the ship owner and manager.

Session 2: Harnessing Maritime Cyber Resilience

A look at maritime cyber security, safety and risk: This expert led session will look at how the industry is reacting to the advent of increased cyber threats borne out of the growing use of cloud and IoT applications, the number of devices used, and larger ships but fewer crew - meaning even more reliance on automation and remote monitoring. The Forum will discuss what policies, guidelines and best practices are already in place, and how the industry can identify, quantify and mitigate cyber risk. We will also ask if there is a gulf between perception and reality, and what are the real business risks?

Session 3: The Big Data Revolution

How big data usage and management is expanding the boundaries of smart shipping – and how can we harness this disruptive influence to build a real business case and lasting legacy.

Transformation, digitalization, disruptive influence, innovation. These words and phrases are being used more and more and being held up as the drivers of all change and development – not just in our sector but across industry. But what do they mean, and what can they do for us in the shipping sector? We know that the maritime sector is on the cusp of dramatic change – how can we harness all this data and information to build our own businesses and make them smarter, safer, and more sustainable? What value can shipping companies take from the launch of collaborative platforms and ecosystems?

Speakers and Panellists will be announced soon

Event:	Digital Ship Maritime CIO Forum Tokyo
Date:	Wednesday, 30 August 2017
Venue:	KAIUN Building, Tokyo
Website:	https://www.tokyo.thedigitalship.com/
Contact:	cathy@thedigitalship.com

HEAD OFF RANSOMWARE

Patching - software providers will release patches, use them!

Control code execution – Change setting to prevent macros from executing.

User control – Do not let users install software without authorisation.

Filter web browsing traffic - Use a security appliance or service to proxy your outgoing web browsing traffic.

Control removable media access - prevent ransomware from being brought in.

Back it up - Have a backup of your data.

For more detailed information see: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware

JOIN IN AND HAVE YOUR SAY ON CYBER...

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 look forward to the next issue where we will once again analyse the current state of play in shipping and bring you some top tips for staying secure online. Together we can help the industry to Be Cyber Aware at Sea.

PROTECTING AGAINST RANSOMWARE ATTACK

Novae
LOOKING FORWARD

TALKING CYBER SENSE: Jacqueline Spencer-Sim, Class Underwriter at Novae Group talks about the lessons of the "Wannacry" attack.

On 12th May 2017 the devastating WannaCry ransomware attack struck a number of high profile organisations. Over 200,000 computers across 150 countries were affected, from the NHS in the UK, to Renault in France and Megafon in Russia. Yet the attack was not an advanced or a persistent attack. Yes it was coordinated but it was indiscriminate, highlighting that no industry, marine included, is immune from the cyber-threat.

There has been a shift in the nature of cyber-attacks and the threat is evolving. We are seeing more examples of attacks where hackers are attempting to take control of operational and industrial control systems and this is a key threat affecting the marine industry, particularly as today's onboard operational technology (OT) and information technology (IT) systems are becoming connected like never before. If the WannaCry attack had become rife in the marine industry, we could have seen the virus spread across operational databases causing potential loss of hire to vessels and significant business interruption.

So what can companies do to prepare and protect? Our research with Oxford University on the effectiveness of cyber-risk controls establishes the following strategy:

1. **INVENTORY OF DEVICES & SOFTWARE:** Create an accurate inventory of assets that need protecting.

2. **SECURE CONFIGURATIONS FOR HARDWARE AND SOFTWARE:** Update operating systems and applications on software when instructed to do so as they contain important security updates and bug fixes. This is not always possible when there is no budget and operations are stretched but if this is the case, further controls MUST be applied, such as segregation and access control.

3. **MALWARE DEFENCES:** Always have up to date anti-virus protection on IT systems and mobile devices. The free up-to-date anti-virus would have detected the WannaCry virus and blocked it from running.

4. **DATA RECOVERY CAPABILITY:** **B**ack up, back up, back up! Adopt the 3-2-1 backup rule; have at least three copies of your data, store on two different media and keep one offsite or at least offline.

5. **EDUCATION:** Secure the human. Educate end users on understanding basic techniques to prevent incidents in the first place. Train employees to identify common online threats such as phishing, spam and suspicious attachments. Ransomware always involves a human to introduce it to the system.

The WannaCry attack should serve as a wakeup call for organisations, highlighting that more needs to be done to ensure they implement the most basic critical controls. Businesses have an obligation to protect their systems so should ensure they have the necessary security infrastructure and insurance structures in place.

https://www.novae.com/

FAREWELL TO A FRIEND: GILES NOAKES

We were extremely saddened to read of the unexpected passing of Giles Noakes last month. Giles was Head of Security at BIMCO, and made a significant and lasting contribution to the development of maritime security across the industry. Not just physical security, Giles was a leading light in cyber too.

He was well known and highly regarded, actively and expertly advising shipowners, operators, shipping associations, military, non-governmental organisations and government departments on maritime security issues. He was particularly instrumental in the development of Best Management Practices for protection against Somalia based piracy. Giles was 62, and leaves a partner and 4 children.

Mr Philippe Louis-Dreyfus, BIMCO President & Chairperson of the Board said: This is tragic news, we send Giles' family our very sincerest condolences, Giles was a wonderful man and I was happy and proud to have worked with him at BIMCO. We all share his family's sadness, they are in our thoughts at this very difficult time. Giles will be sorely missed by all who knew him. BIMCO has established a book on condolence, see www.bimco.org for details.

COMPANY SECURITY OFFICERS WORKING TOGETHER

The CSO Alliance has been working for several years with a selection of partners to develop an anonymous cyber-crime reporting portal which meets and exceeds exacting and wide ranging maritime industry needs.

Mark Sutcliffe, Managing Director informed Phish & Ships "The project is running to schedule with announcements in a few weeks and a pilot project ready for testing in the summer, we have been working on this project for a long time and this will be a significant development for the global marine industry".

Jordan Wylie, founder of the Be Cyber Aware At Sea campaign also commented; ""Reporting cyber-crime at sea is crucial so we can understand the extent of this new and complex threat. The safety, security and financial risks to operations are significant and it is time to do something about it before it's too late. We have been working hard for the last year on raising awareness and have made progress but now we must start looking at solutions such as training our crew, implementing procedures and reporting cyber-crime"

To find out more about the CSO Alliance initiative visit their website, www.csoalliance.com

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our Supporters