#9

AUG:2017

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

CSO ALLIANCE
MARITIME

LEARNING CYBER SECURITY LESSONS

Welcome to issue 9 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".

With the fallout of the Petya ransomware attack still being felt across the industry, it has been a very busy time within the maritime cyber security domain. Inside this issue we look back at that attack, and see what lessons have emerged.

Also this month, with the release of updated guidelines, we look at the work being conducted by major shipping trade bodies, and also the United States Coast Guard.

With so much information washing around, sometimes a different approach is needed. As such, we have been pleased to work with expert training film makers, Fidra Films to launch a new video to stress key messages on cyber security.

We believe the "Be Cyber Aware At Sea" film is set to be a vital tool in helping the shipping industry deal with cyber threats. See the article below to download the video and please share with others.

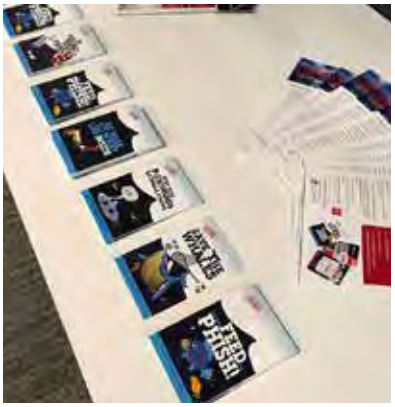
"Be Cyber Aware At Sea" is now also an award winner. We scooped the Cyber Awareness Plan of the Year at the 2017 Cyber Security Awards. Our initiative won for the poster campaign we have been running, which was described by judges as "excellent, innovative with a slice of humour too"!

The awards were established in 2014, to reward the best individuals, teams and companies within the cyber security industry. Excellence and innovation are core themes, throughout all categories, so we were doubly pleased to win amongst such highly regarded cyber security peers. Winners were announced at an awards ceremony held in London.

The win is recognition, not just of the campaign itself, but of the support we have received from industry. So thank you, and please make sure you spread the posters far and wide. See https://www.becyberawareatsea.com/ for more details.

We hope this latest issue of Phish & Ships provides further insight into the issues, and helps you and your staff to become cyber aware. Share this newsletter, talk about the issues and stay safe.

Jordan Wylie at the film launch



CYBER MOVIE

Be Cyber Aware At Sea has collaborated with Fidra Films to launch a new film which aims to highlight the vital and increasing importance of cyber security across the maritime industry. The project has been supported by The Standard Club, along with NSSLGlobal, a global maritime satellite communications provider, Oil Companies International Marine Forum (OCIMF), the CSO Alliance and Teekay.

The film, which received its premiere in London recently, uses real-life case studies to highlight how easy it is for cybercriminals to target individual employees. It is people who are often the weakest link in the security chain, from crew and officers, and even shore executives: All can fall foul of cyber criminals. The video hammers the message home.

Sadly, lots of people still fail to spot the signs of simple phishing emails, and accidentally give away secure information to hackers via email or social media. Even something as simple as charging a phone using the ECDIS could allow hackers to gain access to the ship's navigation system. The video therefore focuses on tips to avoid being a target for cyber criminals.

Please distribute it to your fleets, have your managers and staff ashore watch it today, and reinforce the vital message on maritime cyber security. The video is freely available on YouTube and is receiving rave reviews across the industry, so check it out today. https://goo.gl/jE1Nsp

USCG ADVICE

The US Coast Guard has made available a draft Navigation and Inspection Circular (NVIC), asking ship operators to assess their vulnerabilities to cyber attacks, while providing additional recommendations to reduce cyber risk to maritime facilities.

As highlighted in the USCG Cyber Strategy, cyber security is one of the most serious economic and national security challenges as the maritime industry continues to increase use of cyber technology.

The purpose of this draft NVIC is to lay out a series of policies and procedures to mitigate these risks while ensuring the continued operational capability of the nation's MTS", explained USCG.

The circular comes after the Petya cyber attack that hit the giant containership company Maersk, in late June, and affected port operations around the globe. The USCG document can be accessed here https://goo.gl/xAp4jb

Source: USCG

MAERSK MALWARE

WHAT DO WE KNOW?

On the morning of 27 June Richard Carthas, senior director of operations for the APM Elizabeth terminal in New Jersey, received an email warning of a potential attack that morning: "Five or 10 minutes after that, our gate computers literally shut down".

The Maersk Group and their subsidiaries had had little time to fend off the 'NotPetya' virus. Online cargo booking was crippled, with staff forced to rely on personal email accounts and manual processes while the systems were shutdown and restarted one by one.

Since the incident, Maersk has struggled back into full working order, although still facing the PR hangover that is an inevitable by-product. We now have a slightly better idea about the incident: "NotPetya" was ransomware but experts now believe that the motivations behind the attack were not strictly financial but more likely to provoke global havoc. That it was more likely state-sponsored activity certainly colours things – these hackers can be better financed and more technologically savvy than your regular commercial criminal.

However, that does not negate the responsibility of all industries to protect themselves and their customers as best they can against attack. Indeed, if your shipping line can fall prey to an effectively random virus with such damaging results, imagine how potentially worse it could have been if it had been targeted.

WHAT SHOULD WE CONCLUDE?

The overwhelming message from the cyber security sphere in the wake of this incident is that the industry is by no means prepared enough. Studies released in July by maritime analyst SeaIntel concluded that 44% of the top 50 carriers have weak cyber security. The problems ranged from weak passwords, security patches not updated frequently, and a failure to use encrypted web browsers. They even found one computer server running on a 14-year-old Windows which could be easily entered using a tool downloaded from the internet. As Lars Jensen, CEO of SeaIntel confirmed, "The individual weaknesses found might not be severe in themselves, but collectively [they] indicate an industry with a disturbingly low level of cyber security."

Jensen's most clear conclusion is that no system can provide 100% security from a virus. Systems in international firms of this size are just too heavily interconnected and personnel risks extend from multiple offices worldwide to sometimes necessarily allowing access to third parties to their systems: "This makes it difficult to get a consistent external perimeter in the cyber landscape."

LOOKING FORWARD – HOW SHOULD WE REACT?

The reality is that all players in the industry must invest in their cyber security, from hiring specialized consultants, inputting stricter data controls and checking their insurance includes cyber threats, to top to bottom training of staff to minimise preventable intrusions. Peter Tirschwell writing for IHS Markit compares it frankly to "airport security; these are necessary costs that can never be 100% effective, but that in the end are just that – costs, not investments."

His sentiments are echoed by Mike Simon, principal consultant with DefinedLogic: "It's a shame that so much energy and recourse will have to be dedicated to something that doesn't add any intrinsic value." Perhaps these costs are best seen as a form of insurance to protect against the undeniable costs of suffering a cyber attack; 'NotPetya' caused $US850 million in economic costs according to risk-modelling firm, Cyence and they believe there is potential for further attacks to cost billions.

Mike Simon also drew attention to the elephant in the room that all organisations must contemplate as they model themselves for the future – that advancing digitization in the industry, by definition, necessitates greater exposure to cyber threats. As Mike outlined: "They go hand in glove. For every new process that you are automating or innovating, it will be necessary to put the other hat on and look at how someone can compromise this."

Organisations must resist burying their heads in the sand about neither the positive impact that technological progress has, nor the threats that it exposes them to. Holding back against the technological tide is not a realistic option for companies already playing catch up; instead they should see this time as an opportunity to build their interconnected systems with cyber security within the foundations rather than as an afterthought.

This incident is the warning shot across the bows that the industry required to put its house in order. Now it must make the necessary changes, and fast, to protect themselves and their customers.

source:maersk.com

BIMCO UPDATES ITS CYBER GUIDANCE

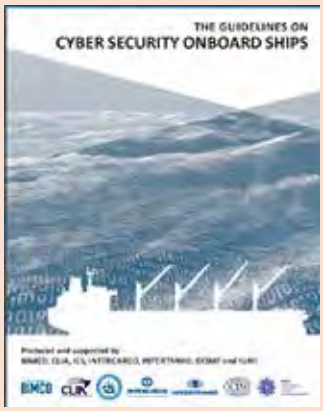
BIMCO has launched their updated guidelines with Cruise Lines International Association (CLIA), the International Chamber of Shipping (ICS), Intercargo and Intertanko, to help the shipping industry deal with cyber-attackers.

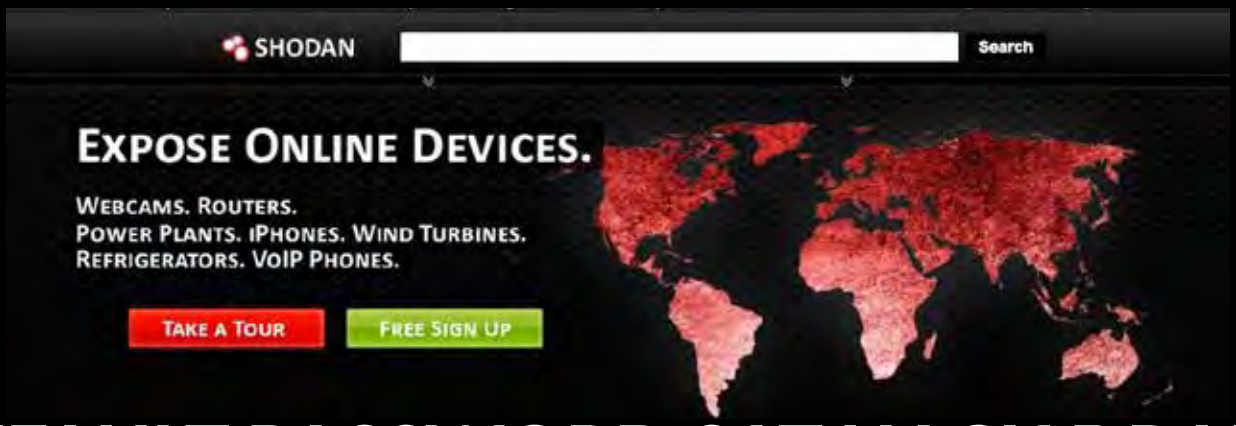
The Guidelines on Cyber Security Onboard Ships are a free to download resource and available from the partner organisations. These guidelines continue to outline the many cyber vulnerabilities which can affect shipping companies, and there are details of steps which can be taken to reduce the threat.

According to the report, bridge and navigation systems including ECDIS, GNSS, AIS, VDR and Radar/ARPA, as well as cargo management systems and propulsion monitoring systems all interface with shoreside networks, leaving them vulnerable.

"BIMCO has led the way to identify potential cyber vulnerabilities for ships – and their implications – based on the latest expert research," said Angus Frew, BIMCO secretary general. "The aim is to provide the shipping industry with clear and comprehensive information on cyber security risks to ships enabling shipowners to take measures to protect against attacks and to deal with the eventuality of cyber incidents."

The guidelines can be accessed at https://goo.gl/VbGYGb





DEFAULT PASSWORD SAT HACK DRAMA

In a widely reported cyber incident, vessels recently had their communications systems hacked by a "researcher", and the industry was shocked by how easy it all seemingly was.

Using the Shodan search engine, ships with "Very Small Aperture Terminal satellite (VSAT) communications systems" were found and accessed. Incredibly, the route in was via default login information available on the internet.

Some have described Shodan as a search engine for hackers, and have even called it "the world's most dangerous search engine". Unlike other search engines, it looks for specific information that can be invaluable to hackers. Since almost every new device now has a web interface it is possible to access innumerable web-enabled servers, network devices, home security systems, and even shipboard systems.

Shodan can find webcams, traffic signals, video projectors, routers, home heating systems, and yes, even maritime VSATs. If it has a web interface, Shodan can find it, and that is very worrying indeed.

The discovery was announced on Twitter by @x0rz (https://twitter.com/x0rz), and on finding that access was possible, he could not contain his excitement. "Duuuuuude, default creds everywhere," he posted on Twitter. Adding that he managed to connect with administrator privileges to the ship.

Once the VSAT is infiltrated, an attacker can easily view call logs, upload firmware and modify system settings. Moreover, the VSAT system can be connected to other devices onboard and used as a gateway for access to any vessel's wider onboard network. This could potentially allow a hacker to cause considerable damage.

Lars Jensen, the founder of CyberKeel, called it a hack "born of stupidity". Many in the industry expressed frustration on learning that vessel owners had installed VSAT equipment, but not bothered to change the default factory settings. Jensen stated that "There is only one technical term appropriately describing such an act, and that is stupidity".

Examples such as leaving a password as "12345", would surely count as gross negligence in the event of an accident? There can be no justification for such a dereliction of duty. As one might expect, the satellite communications provider at the centre of the incident was quick to lay the blame squarely on the client.

The company claimed that terminals are delivered with default administrative credentials such as passwords, as is customary with most communications hardware. They went on to add that VSAT users are urged to change passwords during the installation and frequently afterwards in accordance with general password "best-practice" processes.

While it may well be standard practice in the communications industry to deliver products such as VSAT with default credentials, surely there needs to be a better way? Relying on clients to start the security process seems like an invitation to fall at the first hurdle, as has been clearly illustrated.

If a vessel operates with a VSAT system using factory settings, it is imperative they are changed immediately, and that processes, procedures and means of managing passwords are in place on the vessel and within the company.

After all, it's as easy as 123... if you don't change your passwords.

NO MORE RANSOM!

Law enforcement and IT Security companies have joined forces to disrupt cybercriminal businesses with ransomware connections, and are offering a glimmer of hope for those who have fallen prey to criminals demanding a ransom after encrypting data.

Ransomware is malware that locks computers and mobile devices or encrypts your electronic files. When this happens, users can't get to the data unless they pay a ransom. However, even when a ransom is paid, access is not guaranteed and the campaign urges those affected never to pay!

The "No More Ransom" website is an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre and two cyber security companies – Kaspersky Lab and McAfee. Their goal is to help victims of ransomware retrieve their encrypted data without having to pay the criminals.

Since it is much easier to avoid the threat than to fight against it once the system is affected, the project also aims to educate users about how ransomware works and what countermeasures can be taken to effectively prevent infection. The more parties that support this project the better the results can be. This initiative is open to other public and private parties.

With ransomware, prevention is better than cure as unfortunately, in many cases, once the ransomware has been released, there is very little which can be done unless there is a backup or security software in place. However, the good news is prevention is possible and following simple cyber security advice can help you avoid becoming a victim of ransomware.

For those who do fall victim to ransomware, this site offers the possibility to help them regain access to their encrypted files or locked systems without having to pay. They have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

So, if you need help unlocking your digital life without paying your attackers, then the No More Ransomware site should be your first call. https://goo.gl/TkUtdy

MALWARE: THE DELIBERATE AND INDISCRIMINATE THREAT

Novae
LOOKING FORWARD

In our "**Talking Cyber Sense"** series, Sharif Gardner Cyber Unit Training Manager at Novae Group looks at how to tackle malware threats. He urges us to go back to basics.

Events over the past month should act as a stark reminder that the deployment of most cyber-attacks is deliberate and non-discriminate. The world is becoming increasingly governed by technology and without it, businesses are forced backwards.

The full impact of the 'NotPetya' cyber-attack on businesses globally is not yet known, but, there will be losses; millions of dollars of losses. These losses will include the cost of IT forensics to identify the extent of the damage, costs to restore, repair and replace damaged data and programs and wide-scale business interruption loss due to ongoing downtime. The 'NotPetya' cyber-attack, which occurred on the 28 June, affected all business units at shipping giant Maersk who, in an advisory note issued on the 12 July, acknowledged that the system outage had impacted their ability to release cargo from the June 27 – July 9 and that customers could still encounter delays.

What does this mean? Data breaches via third parties are a growing threat and one that is particularly challenging for businesses to protect against. 'NotPetya' was particularly deadly due to its ability to piggy-back onto Ukrainian accounting software. Maersk, for example, was not directly hacked; it was a third party supplier in this case. This was a critical piece of accounting software that streamlined payment and accounting functions and organisations were auto-running this software to avoid clunky human interaction. This enabled the programme to run as a whitelisted software, thus downloading and running automatically while avoiding commonly used security practices. As a result, this malware spread like wildfire through flat networks and forced affected organisations back to using manual systems, leading to inevitable delays.

What should you do? Third party vetting is essential to protect against this type of malware. Ask your business these questions: Strategically

- Which third parties are providing a service that is critical to operations?
- What security MUST we expect from these suppliers?
- What is our legal, forensic (accounting), PR and insurance response?
- What is our business continuity plan for operating without the use of IT?

Businesses must continue to take these essential preventatives steps:

- Always patch operating systems and software applications. Whilst traditional signature based anti-virus doesn't pick up new strains of malware, it will protect against known viruses
- Always have anti-virus programmes set to run regular scans of systems and emails. Heuristics based anti-virus software will provide more protection if the malware is previously unseen.
- Separate networks where possible to reduce the vast spread of malware.
- #BeCyberAwareatSea 'Don't feed the Phish'. Avoid clicking on malicious links

https://www.novae.com/

OUTRUNNING OUR UNDERSTANDING

Classification Society ABS has been commenting on the maritime latest cyber attacks. In their view, there are signs that the industry is at a worrying point, with technology "outrunning system understanding".

While automation systems on ships and offshore assets have brought with them many advantages, they have created problems too. Not least the fact that these systems are often vulnerable to specific errors, failure modes or intrusions. To keep these systems safe and operating as they should, ABS has developed a list of minimum requirements for maritime cyber security. According to their new ABS CyberSafety® program:

- The right system architecture is required
- Incident response and recovery capabilities are vital
- Software management is key

These three factors all provide inputs to underpin a risk assessment which, after the decision taken at the IMO, means cybersecurity risks will be required as a part of conventional risk management approach.

That risk assessment process will include cyber-enabled systems and the potential hazards and impacts of certain conditions.

ABS further stressed that shipowners should:

- Establish control systems management to document and understand company or installation systems;
- Develop a Functional Description Document (FDD) to combine system documentation, architectures, networking implementations, failure mode analyses and test results into one place;
- Develop and implement an Incident Response and Recovery capability;
- Develop and implement an effective Software Management of Change process to track and manage assets and software; and
- Put into place a Cybersecurity Management System (CMS) that allows the company to understand their current posture and their prioritised actions to address risk factors or risk conditions.

ww2.eagle.org

Sponsored by:

CSO ALLIANCE MARITIME

www.becyberawareatsea.com

think@becyberawareatsea.com

With thanks to our many industry supporters....