MARLINK
Connect smarter. Anywhere.

Contents:

Cyber Security

Next generation defences against the growing threat of cyber-attacks

Checklist

Is your business secured in the digital age?

Assess your end-to-end network architecture and tick the boxes for solutions currently implemented in your system. Marlink is available to provide guidance on how to close any identified security gaps.

Prevent	☐ Secure Network Architecture (Corporate / Leisure LAN Split, Corporate VPN, etc) ☐ Periodic Network Audits of IT infrastructure (Penetration Testing) ☐ Software Update Management System
Protect	☐ Gateway Firewall ☐ Onboard Firewall ☐ End-point Anti-Virus ☐ IT Charter / Usage Policy ☐ User Access Management ☐ Website Category & Content Filtering
Educate	☐ Staff Training on Cyber ☐ Clearly communicated cyber-attack Contingency Plan
Detect	☐ Next-generation Threat Detection (including: Deep Packet Inspection, Intrusion) ☐ 24/7 Security Operations Centre Support ☐ GDPR Risks assessed, cyber-attack response plan to meet 72 hour window
Respond	☐ Automated regular onboard critical system back-up & quick restoration ☐ Secure Remote Access to all machines onboard

Introduction

In 2017 alone, successful cyber-attacks cost the maritime industry hundreds of millions of dollars. Preparing and implementing stringent cyber security standards is essential to mitigate the effects and potential loss. As a satellite communications, IT and digital solutions provider, we take our role in helping our customers to defend against cyber-threats very seriously and provide a range of solutions today to reduce the risk of a cyber attack and mitigate the consequences.

While technology is important, education and understanding are key. In this white paper we aim to explain the challenges, the methods that cyber criminals use and the solutions and technolgies in place to prevent cyber attacks. Ultimately, successful cyber security is a collaborative approach and Marlink is committed to helping its customers to protect their vessels, staff and business.

It is worth noting that so far most known large-scale cyber-attacks in the Maritime sector have been untargeted (including WannaCry and NotPetya). However, it is widely expected that cyber attackers will increasingly "discover" the Maritime industry and launch targeted attacks which are much more dangerous and can only be detected using next-generation cyber security measures.

Rapid Satellite Capacity Growth and Vessel Digitalisation

For many decades, ocean-going vessels were connected via voice and low-bandwidth communications which was used exclusively for business purposes (e.g. communication with shore office, port authorities).

Thanks to the large scale deployment of High Throughput Satellites (HTS) in the maritime sector, the available bandwidth has increased manifold while the cost per transferred megabyte (MB) has decreased. As a consequence, it is widely expected that cost will no longer be an entry barrier leading to twice as many broadband connected vessels in the next 6 years (see figure below).

Already, crew on vessels expect to use communications for welfare purposes (e.g. browse the Internet, chat with their families and friends) and according to latest surveys, for 78% of seafarers this has a strong influence on their choice of employer. Technically impossible just a few years ago, according to the same survey, nearly half of the respondents see 1 Mbps as the minimum acceptable crew bandwidth.

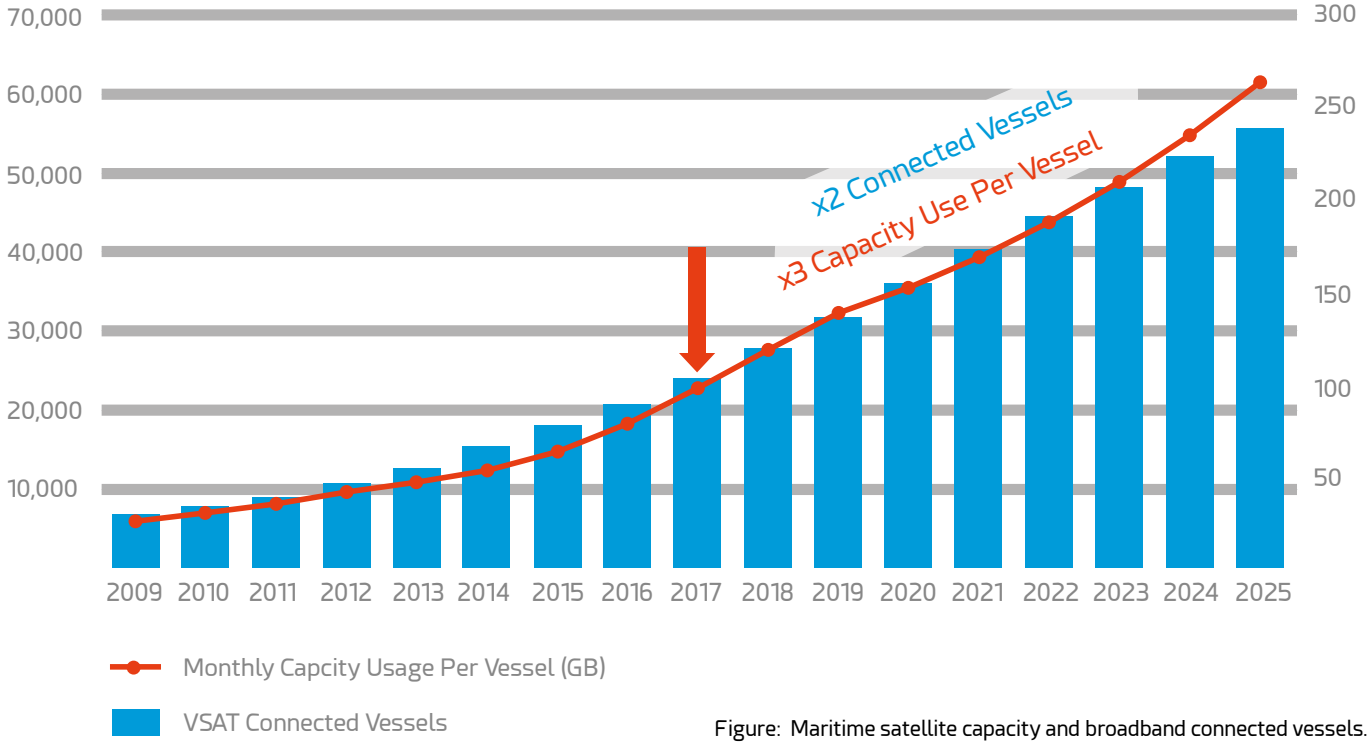

Figure: Maritime satellite capacity and broadband connected vessels.

In addition to enhancing existing applications such as crew welfare, the higher available bandwidth will allow vessel operators to connect their various vessel systems to shore at negligible cost. This will enable digitalisation applications offering increased operational efficiency and optimising processes, such as:

• Fuel & Energy Efficiency:

Transfer vessel sensor data onshore to specialised analysts in order to recommend the most efficient operating processes.

• Environment & Reporting:

Automate emissions data collection and reporting to authorities (e.g. MRV in the EU).

• Smart or Predictive Maintenance:

Manufacturers could detect potential equipment failure in advance and perform corrections via remote connection or schedule an intervention at the next port visit.

• E-Navigation:

Update navigational charts automatically into the ECDIS or remote planning of vessel navigational routes..

• E-Learning:

Update learning material automatically and synchronise crew certificates to the shore HR office while still at sea.

Cyber Security State Of Play

Maritime cyber awareness, a particularly vulnerable industry

The increasing inter-connectivity of vessel systems combined with the growing penetration of broadband communications (e.g. VSAT) and multi-bearer services (e.g. 3G/4G) enables operational efficiency gains, but also increases the vulnerability to cyber-attacks.

Although historically not considered part of the critical infrastructure sector, given the fact that more than 90% of global trade is carried by sea, shipping companies may increasingly become a cyber target. In fact, the Maritime industry is particularly vulnerable for the following reasons:

1) Information exchange across many stakeholders at different time zones

Vessel staff regularly communicate with different stakeholders, such as the ship owner, charterer, origin port, destination port, consignee, customs authorities and bunker providers. This signficantly increases the vulnerability of the communications systems and processes and enhances the likelihood of a hacker attack.

2) Vulnerability of legacy systems onboard

While the modern IT system life cycle is 2-3 years, the lifetime of a vessel is 25-30 years. Security was not a concern when many legacy Operational Technology (OT) vessel systems (e.g. navigational computers, engines) were developed and many are using vulnerable practices (e.g. outdated protocols, default password, static public IP address).

However, many vessel OT systems may not be modified for regulatory reasons and might no longer be supported by the manufacturer. It is therefore crucial to isolate and protect these systems to avoid spreading any OT vulnerabilities to the entire IT system.

3) Low Crew Awareness

Most crews and on-shore staff are insufficiently prepared for cyber-attacks, resulting into behaviour that fails to contain the damage. Crews need to be much more made aware on what are typical cyber-attacks, how to prevent them and how they can contribute to raise cyber security onboard.

Captain, officer and crew are frequently under a high workload with vessel opeational tasks, they cannot and might not see IT securit as a priortity. Furthermore they are more and more carrying their personal devices on-board, accessing more reguarly the internet while at sea, and consequently increasing the chance of infection on the vessel networks.

Dynamic cyber environment

Cyber vulnerability has been increasingly exposed at recent industry conferences and is now seen as an organisation wide concern for IT technicians, ship managers and C-level executives at shipping companies.

Cyber security threats are dynamic by nature and protection against threats is a continuous catching-up. There are over 500,000,000 known malicious programs (malware), with over 390,000 new variations on attacks and new malware detected each day[1]. This mainly covers untargeted attacks with malware indiscriminately sent to as many machines or services as possible, hoping that some of them might become infected.

In addition, targeted attacks by sophisticated organisations with significant resources are becoming more common for businesses. Based on extensive intelligence on the target IT system and the unaware users, the attackers use a blend of customised intrusion methods with the objective of staying undetected in the network as long as possible.

State regulation

When the European Union General Data Protection Regulation (GDPR) comes into force in May 2018, it will be applicable to shipping companies based in the EU, travelling to EU ports or transporting cargo for EU customers. This new regulation forces organisations to take responsibility for data protection and legal liability towards the owner of the data, mandating the notification of a cyber incident to public authorities as well as to the third-party data owners within 72 hours. This regulation requires organisations to improve both their cyber security and develop specialist forensics capabilities or face significant penalties.

Specific to the Maritime sector, the Baltic and International Maritime Conference (BIMCO) has already issued a set of cyber security guidelines, the International Maritime Organisation (IMO) is also working on a best practices document.

The US Coast Guard has created a dedicated Cyber Command unit (USCGCC) and published its cyber strategy in June 2015. While there is currently no obligation to adhere to its recommendations, many industry observers believe that required documentation to enter US ports may soon include an assessment of the vessel's cyber resiliency. A public notification obligation of cyber incidents is already in place in many American states for several years.

Other regions and organisations are expected to follow adopting similar legislation.

Maritime as a target

Actors

The profiles of cyber-attackers have profoundly changed in the last ten years from isolated individuals or small groups operating without a defined strategy to professional criminal or military groups:

• Criminal Organisations:

Traditional organised crime groups (e.g. mafia) have recognised cyber as an opportunity to support illegal trade or to enable financial gain.

• Hacktivists:

Political organisations, underground activists (e.g. Anonymous, LulzSec, Petya) and terrorists are using cyber-attacks to support their political agenda.

• Nation-states:

Nation-states are directly engaging or sponsoring cyber-attacks as a means of warfare and/or (economic) espionage.

• Insider Threat:

An insider threat happens when a person who is close to an organization or has authorized access, misuses that access to negatively impact the organization's critical systems.

 [1]Source : AV-Test.org

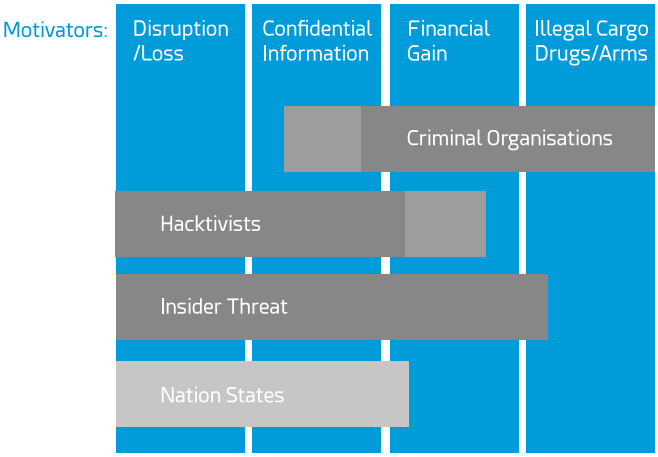

Figure 1 : Overview of actors & motivators of cyber attacks.

Motivations

• Financial gain

To obtain financial gain, cyber-attackers may use 'ransomware', a malicious software rendering a PC inoperative with a demand for ransom payment to unblock it. While most cases are kept in silence, it is believed to be the most common cyber-attack in the shipping industry today. Fleet Managers may feel inclined to give in to the blackmailing as any disruption to business continuity causes direct financial loss and the IT competency of the vessel crew is very limited. However, there is no guarantee that the attackers will actually unblock the computers following a payment.

Another information valuable for attackers are bank details, which may be used to initiate payments to their accounts (e.g. from super yacht passengers, or by counterfeiting bunker fuel invoices). Such attacks are facilitated by the fact that the stakeholders are scattered across multiple time zones and cannot always communicate rapidly.

Criminal organisations or Insiders (e.g. malicious employees with network privileges) are the most likely authors of such attacks.

• Hacktivism

Political groups are increasingly using cyber-attacks as a tool to extract confidential data which is then disclosed to the public to raise public awareness / outcry or damage reputation (e.g. publishing compromising photos taken on super yachts). In addition, political groups may use operational disruption to 'retaliate' against the target's practices (e.g. deactivating or destroying vessel systems).

Common political targets include the Oil & Gas industry, high-net-worth individuals and certain fishing segments (e.g. whaling). Organisations could potentially also make use of cyber-attacks to cause damage or even loss of life to support their objectives. Hacktivists are not typically interested in financial gain.

• Mafia / Smuggling

As opposed to the previous two motivations, criminal organisations aiming to transport illicit goods (e.g. drugs, arms, etc) are generally aiming to stay undetected. An interesting example is the Antwerp port cyber-attack[2] in which drug traffickers recruited hackers to gain access to the IT systems controlling the movement and location of containers. This attack demonstrates the sophistication and resources of organised crime related to cyber-attacks.

• Piracy

While there has not yet been any reported case of physical piracy supported or prepared by a cyber-attack, theoretically a vessel could be led off course or taken over by pirates through an engine shut down or by taking over the navigation systems on board.

Cyber-attack impacts

Safety risks

While most current vessel systems are not yet connected to external networks, it is widely assumed in the maritime industry that in the decade ahead the optimisation of processes and operations will drive the digitalisation of the maritime sector. This evolution may result in additional vulnerabilties, caused by human beings:

 [2] Source: BBC Article (http://www.bbc.com/news/world-europe-24539417.

• Critical systems interruption:

Piracy attacks could be facilitated by deactivation of vessel engines, falsified navigation charts.

• Vessel Hijacking:

Controlling a vessel remotely, attackers could try to provoke vessel collisions, shore accidents or move containers (e.g. using the vessel's crane).

A glimpse of the potentially disastrous possibilities is offered by a 2015 attack on a Remotely Operated Vehicle (ROV): a hacker was able to override the controls sent from the mothership to the ROV, causing the ROV to sink to the seabed[8]. The cost of the resulting salvage operation was $500,000.

Fines by authorities

In the past, national data protection agencies' maximum fines for non-compliance used to be a very limited deterrent (e.g. €100k in France and €900k in Spain). However, under the new EU GDPR regulation, non-compliance can lead to potentially substantial fines of up to €20m or 4% of annual global company revenue (whichever is greater). Moreover, the EU has indicated that penalties will be particularly severe if a cyber-attack was facilitated by negligence (e.g. insufficient protection mechanisms, unencrypted sensible data, untrained staff).

Insurance

Maritime insurance companies have recognised the risk of cyber-attacks and refuse to provide coverage if the damage was a consequence of it. Therefore, virtually all maritime insurance policies contain the Institute Cyber-attack Exclusion Clause (CL380 – see Annex 1). Many shipping companies are probably unaware of this financial risk and would be unable to absorb this potentially huge liability. Taking the case of the 2007 loss of the MSC Napoli as an example (although not caused by a cyber incident), overall liabilities linked to hull loss, cargo loss, environmental damage, personal injury and removal of the wreck came to over $1 billion[3].

Business disruption

Business disruption as a result of a cyber-attack is another source of potentially considerable financial impact. The 2011 attack on the Islamic Republic of Iran Shipping Lines (IRISL) gives an idea of the potential scale: the cyber-attack caused an outage on the entire internal network, meaning rates, loading, cargo number, date and place were not available[4]. Consequently, a number of vessels had to stop operating as cargo manifests were inaccessible; in a number of cases, cargo was sent to the wrong destination and had to be recovered, causing additional losses. Such an outage affecting the entire 115 tanker fleet might have caused direct losses of over $1m / day[5].

The financial risk for cargo operators is even higher; in 2017 the average cargo operator's capacity was 100,000 TEU; meaning that the potential direct loss of an IRISL-like fleet-wide attack would be $100m / day[6]. Considering the strained financial situation and cyber exclusion clause in most insurances (see Annex 1), many cargo operators might not be able to financially sustain such an attack.

Connectivity outage resulting from a cyber-attack may also cause disruption on a smaller scale, e.g. by non-timely reporting of Notice Of Arrival and Departure (NOAD) forms for port entry:

- Delays for entering into port
- Fines by authorities for non-timely / non-electronic reporting
- Late cargo delivery penalties
- While waiting for port entry: additional fuel burnt, additional crew working & vessel charter days
- If the issue cannot be resolved remotely: travel expenses to send IT technicians onboard.

 [3] Source: Allianz Safety and Shipping Review 2015. [4] Source: CyberKeel Whitepaper "Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas" 2014. [5] Assuming direct operating costs per vessel of $9,000 / day. [6] Assuming operating costs of $1,000 per TEU. [8] Source: Marine Electronics & Communications Article "Shipping unprepared for five stages of a cyber-attack".

Company reputation

Less immediate than the previously mentioned consequences, the negative impact of a cyber-attack on a company's reputation can however be substantial in the longer term. In a survey by the Economist Intelligence Unit in 2016[7], C-suite members of large companies were asked about the greatest risk of a cyber-attack; the majority responded: damage to "our reputation with our customers".

While it may take decades to build trust in a brand, media coverage about a cyber incident amplifies a negative association, which can severely damage the public reputation for a long period of time. Consumers and businesses are particularly sensitive to cyber breaches because it exposes the confidential data they have entrusted the company with (identity, bank details, business information) and may lead to financial losses.

Critical maritime protection solutions

The Maritime industry has only recently started to understand the risk to its assets and the need to protect critical systems. Cyber-attacks to critical systems as outlined may disrupt business continuity (e.g. connectivity outage) and paralyse a vessel.

The direct and indirect cost factors of any such delay to the voyage are extensive. Rather than being an isolated IT topic, all concerned stakeholders (including finance, fleet operations and commercial departments) need to draft a contingency plan with response procedures in case of a cyber-attack.

A risk assessment of the vessel's critical systems and contingency plans need to be established. For instance, the GPS position and ECDIS charts are fundamental to the ship's navigation and safety, yet experts have demonstrated that many systems suffer from cyber vulnerabilities.

Moreover, the cargo manifest can be of high value to attackers seeking to read or modify the information to enable illicit trade. Secure network architectures are emerging which isolate systems identified as critical to vessel operations (ECDIS, ERP Systems, etc) from directly facing external networks.

Implementing a back-up communication system which could be non IP-based and has a different entry point would allow business continuation in case of a major infection of all IP communication systems.

 [7] Source: Economist Intelligence Unit "The cyber-chasm" 2016.

Cyber Attacks & Security in a Nutshell

Methods of intrusion

Untargeted attacks:

Every cyber-attack is composed of multiple phases, the first one being intrusion into the network. The following untargeted intrusion methods are indiscriminately sent to as many machines as possible:

- **Email threats:**

Many of the most prolific viruses distribute themselves automatically by email. Any attachment received by email could carry a virus; and launching such an attachment can infect a computer. Even an attachment that appears to be a safe type of file, e.g. a file with a .txt extension, can pose a threat. The amount of email spam and viruses is rising constantly and are estimated to represent more than 70% of global email traffic.

- **Malware Apps on Personal devices:**

With more and more personal devices of seafarers (Bring Your Own Device = BYOD) being used on a vessel's network, apps containing hidden malware can provide a backdoor for cyber criminals.

There are currently at least 7000 free apps proven to contain aggressive adware that can lead to an infected IT network. 80% of them are still available on app stores. The potential for infection is high as over 10% of these have been downloaded a million times.

- **Worms:**

Rather than direct infection, a PC could also become infected by a worm creating exact copies of itself and using connectivity between computers to spread within a network.

- **Keylogger:**

Using a hardware device or covert software to record every keystroke and mouse movement made by a user, cyber-attackers may extract confidential information or passwords to gain access to IT systems.

- **Brute Force Attack (Weak Passwords):**

A trial-and-error method using automated software to guess a user password by systematically trying all possible passwords. Such attacks may be prevented by limiting the number of attempts to enter a password, introducing time delays between attempts and strong passwords (minimum of 12 characters using both alphanumerical characters and symbols).

Targeted attacks:

In a targeted attack, attackers initially perform extensive intelligence on the specific configuration of the IT system as well as its vulnerabilities or on the people using the systems and then tailor malware specifically to an organisation. Most conventional cyber security measures (e.g. anti-virus, firewall) will not detect such specifically targeted malware.

• Pharming and phishing (Social Engineering):

All attacks can be supported by Social Engineering based on impersonation techniques, e.g. using a bogus Social Network profile showing the same interests as the person and coming from the same hometown. This is very effective in tricking a person into installing the malware application, opening an email attachment or supplying confidential or personal information.

Another method consists of distributing an email that appears to come from a reputable organisation, such as a bank. The email includes what appears to be a link to the organisation's website. But the link directs to a replica of the website. Any details entered, such as account numbers, PINs or passwords, can be stolen and used by the hackers who created the bogus site.

• 0-Day:

While anti-virus programs protect against signatures of known malware in their threat database, there is a time window between the detection of new vulnerabilities, the time they are added to the anti-virus database, software patches are developed and the time the anti-virus signature update or software patch are deployed on the computer. This very sophisticated method is often used by targeted attacks and can only be detected through behavioural analysis and Deep Packet Inspection (DPI).

• Advanced Persistent Threat (APT):

An attack specifically designed to be difficult to detect using conventional means, thereby allowing the attackers to remain undetected in the network for a long time: more than three months on average[9]. APTs can only be detected using advanced Cyber Detection solutions.

• Intrusion via a less secure / third-party network:

If the configuration of the target's IT system is known, attackers may attempt to first gain access to a less secure (e.g. BYOD device, social network) or a third-party system in order to then intrude into the corporate network. The 2014 cyber breach on the US retailer Target actually started via a breach of the heating and ventilation contractor's billing system.

Malicious Software (Malware)

Once the cyber-attackers have obtained access inside the network; they deploy malware in order to carry out their main mission. Malware can be classified into the groups explained below and, in some cases, actually may belong to several groups (e.g. a Trojan Horse spreading as a worm).

• Trojan Horses:

A Trojan Horse appears to be legitimate software with a clear function (and may even carry it out), but actually performs another task in parallel, usually without the user's knowledge.

• Spyware:

Software that enables hackers to gather information without permission. It tracks activity or copies data and reports it to others, and consumes memory and processing capacity that may slow or crash computers.

• Adware:

Software that displays advertisements on computers. Adware can slow down a PC and is designed to be difficult to uninstall.

 [9] The average dwell time of an infection in a network is 99 days.
Source : Airbus Defence & Space FireEye M-Trends 2017.

• Ransomware:

A type of malicious software which blocks the system or encrypts data, forcing its victims to pay a ransom to the cyber-attackers in order to regain access to their system. Commonly used Ransomware programs include Bit Locker (not to be confused with the Microsoft product) and Locky.

• Remote Access Tool (RAT):

A malware program providing remote control over the target computer to the cyber-attacker (e.g. to take screenshots, activate the webcam, format drivers, access locally stored files).

• Botnet / Zombie:

A group of computers infected with a RAT which is used to carry out malicious tasks (e.g. sending email spam, DoS attacks). In most cases, the owners are not aware of the breach.

• Rootkit:

A piece of software that hides programs or processes running on a computer. It is often used to conceal misuse of the computer or data theft. Once a rootkit is running on a computer, the user cannot reliably identify all the processes running on that computer.

Disruption

Most cyber-attacks perform espionage (Trojan Horses, RAT) or aim to take over IT systems for specific purposes (Ransomware, Botnets). However, some attackers primarily intend to cause disruption:

• Denial of Service (DoS):

An infrastructure attack aimed at making a system unavailable to its intended users by flooding a server with a large number of requests, thereby blocking the fulfilment of legitimate requests.

• Sabotage / Destruction:

In some cases malicious software are aimed at destroying industrial systems (e.g. Stuxnet) or making computers unusable (e.g. by deleting the operating system). A different entry point would allow business continuation in case of a major infection of all IP communication systems.

Conventional Maritime Cyber Security Measures

Cyber security framework

In order to protect a property, one would generally first conduct a study of the grounds and the neighbourhood to identify weaknesses as well as all possible entry points and then install a number of locks and shutters (PROTECT) as well as alarms and sensors (DETECT). In case of a confirmed intrusion, a RESPONSE is performed: one would call the police.

As shown in below Figure 2, this is a continuous process; after an intrusion, one would generally try to understand how it was carried out and improve the means to PROTECT and DETECT.

Figure 2: Continuous cyber security process

In the same way, protecting a Maritime IT network against cyber threats requires a combination of proven tools and processes. Isolated means such as a firewall and anti-virus (PROTECT) need to be complemented by a strategic deployment of threat detection and response hardware and software (DETECT and RESPOND) as well as training of the staff on board. This will help to ensure never being in a position of having to pay hackers a ransom, a fine to national bodies or suffering from a severe loss of reputation.

Staff Awareness & Usage Policy

While access to the Internet for business as well as for welfare to stay connected with family has become common among shipping vessels, many crew members are not aware of cyber risks.

Therefore, in addition to technical cyber security solutions, it is essential to create awareness among the staff through regular training as well as a clearly communicated IT usage policy ('IT Charter'). Cyber criminals know that untrained people or those with little computing experience are an easy target. If malware of any sort does get through to a vessel's PC network, the final step for the attack is the execution by the user which may be facilitated by social engineering.

Training courses should teach best practices (e.g. avoid opening suspicious email attachments), clear procedures in case of a detected cyber-attack as well as awareness about available secondary back-up systems.

Access Management

There are several technical means to implement this policy: The first, and most obvious parameter is user authentication to ensure that the user (a human or a device) is approved to be on the network. Once this is established, user access management can be set based on e.g. specific time slots according to shift patterns. Thanks to this system, it is also possible to detect any unauthorised access attempts, or keep track of usage patterns.

Marlink's XChange Service Delivery Platform includes a complete User Access Management system. (see "Marlink IT & Network Security Solutions" Brochure).

Endpoint Device

Firewall

The first line of perimeter defence is the firewall integrating basic protections and being able to filter Internet traffic upon defined rules (e.g. based on ports, protocols, applications). A shore-based firewall available for all connectivity customers may be complemented by a firewall deployed at the vessel, scrutinising requests from remote terminals to the Internet. This service provides protection against untargeted Internet attacks and non-customised malware.

All Marlink onboard solutions include firewalls (e.g. XChange 2-stage Firewall and Cisco Firewall, see "Marlink IT & Network Security Solutions" Brochure). In addition, Marlink also provides shore based firewalls: Data Manager and @SEAwebControl (see "Marlink IT & Network Security Solutions" Brochure).

Anti-Virus

Anti-Virus software combats a wide range of threats such as viruses, Trojan horses and other malicious software by comparing detected programs to the signature database of known threats. Regular updates are therefore key to detect the most recent threats.

Some anti-virus software providers are complementing signature-based protection with behaviour-based screening; thereby even if a new ransomware software is not part of the signature database it may be detected by analysing its behaviour (e.g. if a process starts encrypting a large number of files).

Marlink provides a satellite optimised anti-virus package including both signature- and behaviour-based screening (SkyFile Anti-Virus) as well as version monitoring of any anti-virus software through KeepUp@Sea (see "Marlink IT & Network Security Solutions" Brochure).

IT System Configuration

Particularly on Corporate PCs, it is recommended to enforce the IT charter through management of the PC's configuration (e.g. through settings in the Windows registry). Depending on the criticality of the machines, measures could include: deactivation of all USB ports, blocking of new devices to be connected or new software to be installed unless an administrator has given prior approval. IT Configuration Systems detect attempted changes to the system and automatically roll back to the latest approved configuration.

Marlink's KeepUp@Sea operational vessel IT platform includes Configuration Management with automatic restoration.

Applications

Email Security

It was reported in April 2016 by security company Retarus that one in six of all incoming emails in the world are blocked because of positives from Anti-Virus software. Malware delivered via email attachments is one of the key transport mechanisms for intruders to get access to an IT network. One potential aspect of email security includes only downloading attachments when they are requested by the email recipient. Of course, this is good practice to save on satellite airtime, but is also important to reduce the number of unknown executable files coming on board a ship.

Marlink's SkyFile Mail solution includes Attachment Protection (see "Marlink IT & Network Security Solutions" Brochure).

Website & Content Blacklisting

A firewall may be complemented by web filtering carried out at various different levels, using specific profiles and additional layers:

• Category filtering:

Restricting user's web access by blocking certain categories such as undesirable content (i.e. drugs, racism or hacking) to non-productive activity (i.e. games) to security threats (i.e. P2P sharing and sites with known malware)

• Content filtering:

Blocking certain types of content to avoid download of potentially harmful files (e.g. exe files).

Filtering policies applicable to a vessel, or groups of users can be implemented. If an attempt is made to access a restricted website from a computer onboard a vessel where content filtering is enabled, the user will be blocked or redirected to a website where information about the policy violation is given.

A combination of both category and content filtering systems is recommended as even white-listed categories might contain unwanted or unsecure types of content (tracking cookies, viruses or malicious software).

Marlink provides website category and content filtering as part of the following two Value-Added Services: Data Manager and @SEAwebControl (see "Marlink IT & Network Security Solutions" Brochure).

System Back-Up & Resiliency

Although Secure Remote Access allows remote secure intervention on a PC, this risks causing excessive satellite airtime consumption. Therefore, for cases of malware infection and ransomware but also to protect against hardware failure, it is good IT practice to implement an automatic back up process to a physical secondary system on-board. Considering the remote aspect of ships, back-up systems enable operations to be restored right away, rather than waiting for a remote technician to intervene or even wait for back-up hard disks to be delivered and installed in port.

Marlink's KeepUp@Sea IT platform includes an automatic back-up and restoration function (see "Marlink IT & Network Security Solutions" Brochure).

Update Management

Software updates are published frequently to include new features, but also to fix security vulnerabilities. Although software updates consume satellite bandwidth and take time, these should be performed regularly to avoid known vulnerabilities in outdated software being exploited by an attacker as a method of intrusion.

The WannaCry ransomware outbreak in May 2017 exploited a vulnerability in the SMB protocol for which Microsoft had released a patch two months before. Despite abundant media coverage, many systems were not updated and the NotPetya ransomware used the same vulnerability in June 2017 to again cause disruption on a large scale. The likely explanation for this is a lack of centralised awareness about deployed software versions across an organisation. Specialised monitoring and reporting software allows a Fleet Manager to see an overview of the deployed software versions on all PCs in their fleet, identify vulnerable versions and launch updates remotely.

KeepUp@Sea includes version management of deployed software onboard (see "Marlink IT & Network Security Solutions" Brochure).

Network Infrastructure

Network Configuration

In addition to protecting against outside threats, to avoid spill-overs, it is also essential practice to isolate networks used for different purposes: The business critical Corporate Network should be clearly isolated from the potentially less secure Crew Welfare Network. Marlink prevents cross-network access by either of the following two methods:

• Virtual Routing and Forwarding Technology (VRF):

Networks are delivered to separate termination points using dedicated VLANs.

• Physically split Local Area Networks (LAN):

Networks are physically separated requiring separate cabling. Additional security settings can be applied to physical networks to prevent non-listed computers and systems from cross-connecting between networks.

Thanks to this implementation, since a Crew PC, smartphone or tablet cannot access the Corporate LAN, untargeted malware cannot spread from the Crew to the Corporate LAN. Moreover, this is a good defence against a targeted cross-network intrusion of the corporate network through a less secure network. However, such network separation can only act efficiently in combination with staff awareness: Despite the separation of Crew and Corporate networks, a crew member could infect a Corporate PC by connecting an infected USB drive.

Marlink's XChange includes network isolation technology (see XChange and Cisco chapters in the "Marlink IT & Network Security Solutions" Brochure).

VPN

To increase security against outside intrusion or eavesdropping when routing through the Internet, an encryption protocol may be used to add another layer of security. However, an encryption method suitable for usage over satellite should be chosen, as some types of encryption are geared towards terrestrial usage and use extensive amounts of bandwidth. Additionally, encryption for user authentication can also improve resilience.

The benefits of using a VPN are numerous. Essentially, using a pre-defined routing path along a public network, it enables a secure extension of an internal network to a remote location. This makes Corporate IT networks more coherent and easier to manage, by including the vessel into the same network as any shore office.

Two types of VPN solutions are provided by Marlink:

• HQ Interconnect:

From the Marlink teleport gateway to the Customer HQ.

• End-to-end VPN:

From the vessel via the Marlink teleport gateway to the Customer HQ.

Secure Remote Access

There are rarely IT specialists on board a ship, so more complex software based issues may require a technician to visit, which is costly and operationally difficult to manage. It is becoming more common for IT management of on-board PC networks to be performed remotely. However, rather than using insecure means such as a Public IP, a Secure Remote Access Tool over a VPN with a single point of access should be used. Considering that for additional security Marlink is operating a private network, such tools need to be compatible with Network Address Translation (NAT) on multiple levels.

Thanks to such Secure Remote Access Tools, all PCs can be accessed from shore to fix specific issues or deploy updates. For instance, should a PC require a clean install of Windows, the process can be managed remotely, without the need for any on-board intervention. Similarly, ransomware could be remedied by a reset to an earlier backup.

XChange includes the Universal Remote Access (URA) feature providing secure remote access to all on-board devices connected to it. Moreover, the KeepUp@Sea platform allows to remotely initiate the reset to an earlier back-up or software reinstall (see "Marlink IT & Network Security Solutions" Brochure).

Next generation Cyber Security Measures

Cyber Detection and Incident Response

While signature-based cyber solutions (anti-virus, firewall, content filtering) and a secure network infrastructure (VPN, LAN separation) are effective against untargeted attacks, in order to provide efficient defence against targeted attacks such as APTs, a cyber detection solution should be implemented.

Typically, network probes would be placed in several parts of the infrastructure performing the following functions:

• Deep Packet Inspection (DPI):

Rather than performing filtering based on a packet's meta data, a DPI system will also analyse the payload of the packet

• Intrusion Prevention System (IPS):

Detects common patterns of cyber-attacks (e.g. large amounts of data extracted to unusual destinations) and corporate policy violations (e.g. detection of applications which should be blocked, e.g. BitTorrent)

• Sandboxing:

A controlled environment to test suspicious files (e.g. attachments from unknown senders) to examine for malicious behaviour; effective in case of 0-day attacks

• Traffic Pattern Monitoring:

Raises alerts in case of deviations from usual weekly and monthly traffic patterns (e.g. applications, volume); although more prone to false alerting than the previous three functions, it is an additional source to detect abnormalities.

Alerts generated from these various systems would be aggregated and assessed by a Security Information and Event Management (SIEM) system. In addition to controlling a number of automated countermeasures (e.g. quarantine suspicious machines), this information is displayed in a dashboard overview to be exploited either by the Corporate Network Administrator or a third-party 24/7 Security Operations Centre (SOC).

Based on their training and experience, the human analysts would choose anomalies to investigate further and in case of a confirmed attack perform the follow-up actions such as:

1. Isolate infected assets
2. Remediation (e.g. cleaning)
3. Investigate incident to determine source of attack
4. Improve protection systems (e.g. add attacker's DNS domain to central firewall DNS blacklist)
5. Raise Staff Awareness (training courses, bulletins)

Rather than implementing a dedicated Cyber Detection system and operating an in-house SOC, a shipping

company may achieve economies of scale by using a central system implemented at the Satellite Communication Provider's gateway.

Secure Content Distribution

Even if Internet is becoming a commodity on vessels, it is recommended for the future to limit direct access to navigation assets. Smart and secure content distribution services already today - acting as DMZ between assets and the Internet - can eliminate risks of attacks and infection, as shown in Figure 3.

Not only all of these critical systems to vessel operations (ECDIS, ERP Systems, etc) should be managed in different network groups, software updates and new content (e.g. new training material, navigation charts) shall be transferred indirectly to vessels using such DMZ principles, performing integrity verification / sandboxing of files while preventing an open and direct access to hackers to these assets.

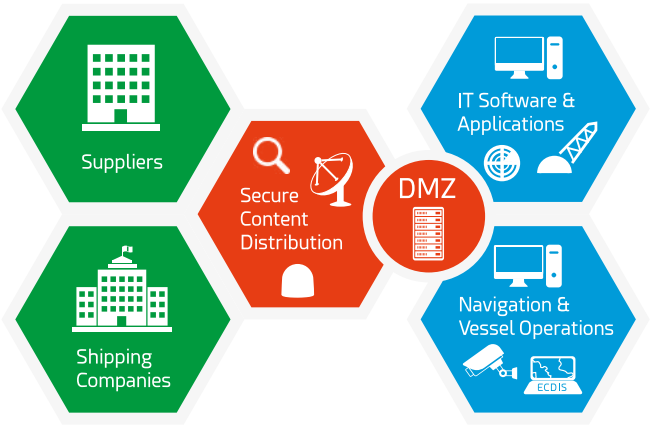

Figure 3: A DMZ-based network architecture to securely distribute content to critical bridge systems (e.g. Radar, ECDIS, ERP Systems)

Consulting Services

As cyber security is a highly specialised and fast moving sector, many shipping operator's internal IT departments may lack the expertise to stay on top of the latest developments. It may therefore be advisable to seek outside expertise for the following tasks:

• Regular penetration tests (pen test):

A white hat attacker attempts to perform an unauthorised intrusion into the tested system without knowing any details about its architecture. The objective is to identify vulnerabilities that could be exploited by malicious attackers, such as flaws in services and applications, misconfiguration or risky end-user behaviour.

• Forensics / Response to authorities:

Many public bodies (e.g. GDPR) do not only mandate companies to inform them in case of cyber incidents but also to analyse which data has been extracted. As attackers often try to hide their trail, this is very time-consuming and requires specialised IT forensics skills (analyse network logs, recover deleted and hidden files, seize RAM data). Moreover, there are several provisions to comply with for the data to be legally admissible in court.

• External Audit of Back-up systems & Contingency Procedures:

It is advisable to ask independent security experts to review the secondary systems and cyber-attack response procedures.

Abbreviations:

APT: Advanced Persistent Threat
BYOD: Bring Your Own Device
DPI: Deep Packet Inspection
DMZ: DeMilitarized Zone
DoS: Denial of Service
ECDIS: Electronic Chart Display and Information System
ERP: Enterprise Resource Planning software
HTS: High Throughput Satellite
IoT: Internet of Things
LAN: Local Area Network
MRV: Monitoring, Reporting and Verification (EU Directive)
NAT: Network Address Translation
NOAD: Notice of Notice Of Arrival and Departure
RAT: Remote Access Tool
ROV: Remotely Operated Vehicle
SIEM: Security Information and Event Management
SMB: Server Message Block
TEU: Twenty-Foot Equivalent Unit (international cargo size unit)
SOC: Security Operations Centre
VLAN: Virtual LAN
VPN: Virtual Private Network
VRF: Virtual routing and forwarding technology

Definitions:

Advanced Persistent Threat:

A sophisticated attack designed to be difficult to detect, remaining undetected in a network for a long time.

Black hat hacker:

A hacker exploiting computer security for personal gain or because of maliciousness

Demilitarized Zone:

A network architecture which only allows external access to certain hosts inside the DMZ (e.g. web services, email server) while the other hosts in the organization are not externally reachable.

Meta Data:

A summary of a dataset (e.g. title, file type, size, modification date, sender, destination).

Payload:

The part of the network packet containing the intended message, i.e.; excluding the Meta Data.

HELO:

A command in an email message containing information about the sender which can be used to filter spam.

White Hat hacker:

An ethical computer security expert who will use information on vulnerabilities to improve the security of an organization's information systems.

Annex 1 - Institute Cyber-attack Exclusion Clause (CL380) (CL 380, 10/11/03)

1.1. Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme malicious code, computer virus or process or any other electronic system.

1.2. Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.

MARLINK
Connect smarter. Anywhere.

Cyber Security

Next generation solutions against the growing threat of cyber-attacks

For more information: www.marlink.com