CYPRUS SHIPPING CHAMBER
Navigates Cyprus Worldwide

VULNERABILITY MANAGEMENT CASE STUDY

(Version 2.0 – May 2018)

Published by
Cyprus Shipping Chamber
City Chambers, 1st Floor, Regas Fereos Str.
Limassol, Cyprus
www.csc-cy.org

Terms of Use

Table of Contents

1. Introduction

There is a perception within the shipping industry that where cyber security is concerned; "it can't happen to us". The implementation of effective cyber security management, especially onboard vessels is a low-level priority and that simple anti-virus protection or that introducing an air-gap between critical systems is adequate.

The truth of the matter is however, that with the rapid increase in digitalization and interconnectedness for all major systems; communications, navigation and automation onboard, ships and their offices are at now at a higher risk of attack than ever.

The well-publicized NotPetya ransomware[1] attack on Maersk in late June 2017 cost the company up to US$300 million. There are many more cyber-attacks that have gone unreported. As well as external threats, vessels are subject to internal attack whether unwittingly through the use of corrupted USBs' for example or through malicious attack by disgruntled employees or crew members.

The Cyprus Shipping Chamber recognizing the need to make the shipping industry aware of the increasing cyber threats both from within and without, has developed this second study on Vulnerability Management to provide guidance to its Members on effective cyber security management.

2. Aim and Scope

Following the same question and answer format as the first case study, but working with a different company on this occasion, this study was prepared to illustrate how a shipping company approaches the concept of vulnerability management both onboard and ashore.

We posed several questions to the company on how they conduct scanning and where they see the biggest challenges on implementing this process into a companywide policy.

The financial considerations involved in improving a company's cyber security posture are also highlighted as to whether shipping companies believe this to be a necessary aspect of their budgeting against what they see as an unidentified and unknown threat cost wise.

It should be recognized that this is not an all-inclusive guidance or evaluation, and does not critically assess their efforts. The intention is to contribute to the greater discussion on maritime cyber security by exposure to a typical case and to find value in their efforts at improving their cyber security posture.

Comments are encouraged to the Cyprus Shipping Chamber to improve this document and to better prepare for future case studies on this subject.

3. What is Vulnerability Management?

Vulnerability Management is a business process aimed at reducing the amount of time a computer or computer-based system is vulnerable to a *known* threat. This then reduces the time a system is vulnerable and thus reduces risk. The process relies on the practice of identifying specific vulnerabilities on target systems and then remediating the issues identified. Identification of the vulnerabilities is typically achieved using a piece of software known as a vulnerability scanner.

At the most basic level a vulnerability scanner examines the subject computer, usually remotely over the network, and attempts to identify the patch levels and versions of the software running on it. The versions are compared to a database of known software vulnerabilities, Common Vulnerabilities and Exposures (CVE)[2] for example. If the subject computer is found to be vulnerable to a known issue it is noted on the report output and given a severity ranking that usually ranges from low to critical. Typically, a critical vulnerability is one that can result in remote takeover of the computer if the vulnerability is exploited.

It should be noted that conducting a vulnerability scan is often referred to as a *Vulnerability Assessment*. Third parties will sometimes include other activities such as examination of firewall rules and router access control lists or ACLs in their vulnerability assessment process but at the core the Vulnerability Assessment relies heavily on the scanning software product. The vulnerability assessment process is separate and distinct from a *Penetration Test* which seeks to closely simulate the outcome of an actual attack. While the VA process seeks to identify specific vulnerabilities on individual computers the Penetration Test seeks to test a larger scope and often includes simulating Phishing attacks and physical access to data processing systems and resources.

While the Vulnerability Management process is fairly straight forward and relies on existing IT Management roles for remediation it is notably more difficult in the maritime environment. While most shore side business networks are patched frequently and often managed in groups the computer systems on vessels are typically more stand alone. This means that when a critical vulnerability is identified IT may have to address the systems individually. This can result in an increase in the amount of time a computer on any given vessel is vulnerable to an exploit.

4. Company Description

Question: Describe your company in terms of fleet size, ship types, number of employees, and number of offices worldwide.

Company Comment:

"Shipmanagement Company with Vessels Trading Worldwide. We have in total over 600+ vessels (Crew and Full management). Shoreside employees are over 1200 persons which includes Crew Manning and Full Technical Operations."

5. Motivation

Question: What are your reasons for implementing vulnerability management on your fleet?

Company Comment:

"Our intention is to comply with recent Marine Organization guidelines for future regulations. With VSAT Installation every crew member has access to the internet. We therefore have to monitor and strengthen vessel networks."

Expert Commentary:

As satellite broadband data rates increase and price plans become more competitive onboard networks will naturally more closely resemble a shore side 'branch office'. In the same way inexpensive network access has transformed almost every aspect of daily life, it will transform operational aspects of maritime vessels. The relative safety of critical systems onboard will be negatively impacted by this. While the threat of USB borne malware is currently the primary concern, expanded access to networked data systems will bring new threats and require mature business processes to manage them. The vulnerability management process, specifically the scanning of systems to determine the condition of networked computers onboard, can be an effective way to reduce the risk of an onboard cyber security incident. This can and should be done in advance of increasing access of onboard systems to the public Internet and other shore-based networks.

6. Onboard Vulnerability Management

Question: Are you presently performing or planning to perform onboard vulnerability scanning or management?

Company comment:

"We are currently using onboard vulnerability scanning of pc's and network."

Expert Commentary:

There are several considerations when determining where and how to conduct network-based vulnerability scans. With VPN access to the vessel network a single scanner can accommodate many vessels or an entire fleet in some cases. This makes performing the scans easier and gives a more overall view of the vulnerability state of the fleet. The down side is the scanner must run all of the traffic across the vessels data connection. Given the amount of traffic a scanner can generate it can impact both network performance and cost depending on what kind of airtime package you are using. The scanner can be tuned to scan more slowly thus reducing the network impact. Scans can also be run during port visits over other wireless networks such as GSM.

Alternatively, the scans can be conducted onboard. This requires that the scanning software is hosted on a system onboard. The software can be hosted on a PC, dedicated appliance or as a virtual machine if the vessel is so equipped. The advantage of this approach is that the scanning traffic is limited to the local network with only the report being transmitted over the satellite data connection.

7. Frequency of Scanning

Question: How often do you conduct scanning as part of your vulnerability management process?

Company Comment:

"We scan our Vessel Network Daily for Vulnerabilities. New vulnerabilities may arise daily."

Expert Commentary:

The frequency of scanning must be carefully considered. The concept of vulnerability management is that the sooner you recognize a critical vulnerability, the sooner you can mitigate it and keep the risk of it being exploited low. In some cases, the networks are only scanned annually and this is too infrequent to have a significant reduction in risk. Generally speaking monthly is a good frequency to start with especially if you are scanning remotely. It is not uncommon for critical systems to be scanned at a higher frequency than non-critical ones. Ideally you want the vulnerabilities identified to be remediated prior to the next scan. If your scan frequency is too low, say once annually, you many never achieve a 'clean' scan as more vulnerabilities are constantly being added to the database than have been remediated between the scans.

8. Detection of vulnerabilities

Question: How quickly or how often are detected vulnerabilities mitigated?

Company Comment:

"It always depends on the vessels' internet connection and whether or not the PC has internet access. If it's an alert that we can remotely fix we will assist at the same time. If it's an issue that needs local assistance from the Captain we will advise the Captain. If it's the case that neither the Captain or our team can assist remotely, then we will send a technician to the next available port to fix the issue. The biggest issue with vulnerabilities may be the updates and on vessels with low data plans we have to update with an internet dongle at the next port."

Expert Commentary:

How often vulnerabilities are detected is a function of how often a vulnerability scan is run. Mitigation is a function of how critical the vulnerability is. A non-critical vulnerability is less urgent and often taken care of with the next update or scheduled maintenance window. A critical vulnerability that puts the subject system at immediate risk should obviously be mitigated as soon as possible. If it is not possible to apply a service patch or perform the required configuration change in a timely manner compensating controls should be devised to offset the risk. For example, if a computer on a vessel is found to be vulnerable to a remote command execution in the browser, use should be strictly limited to trusted sites related to business functions until such time as the vulnerability can be mitigated.

9. Vulnerability Remediation

Question: What are the biggest challenges with onboard vulnerability remediation and how do you address them?

Company Comment:

"Our biggest challenges with onboard remediation is internet access. Most issues would be windows updates or application updates. None of the computers have continuous internet access unless the user connects to the internet with his account."

"We are sending Windows and application updates with update packages on DVD's or sending internet USB dongles to the next vessels for the crews to update the PC's."

"We are testing software that will have a relay server on the vessel and we will distribute the updates from the office to the relay server and then the relay server will update all vessel PC's. This will save us internet access costs."

Expert Commentary:

The most common vulnerabilities detected by the scanning process are going to be related to operating system and application update patches. While in a shore-based business and even

home environments this isn't much of a problem, you simply use the OS or application update process and the problem pretty much takes care of itself. Unfortunately, with vessels it is a bigger problem. Pulling down a Microsoft Windows update over the air is expensive, time consuming and prone to multiple data transfer issues associated with transferring large files over often intermittent networks.

At the time of this writing most ship managers update with removable media such as a DVD. As pointed out in the above reply there are logistical hurdles with this approach. It requires the creation and delivery of the media as well as the assistance of onboard personnel. As a positive effect of the vulnerability process the frequency of this kind of update will increase.

Once you see a critical vulnerability you're motivated to fix it. When you aren't seeing them, before you started scanning, there isn't as much pressure to update. It's harder to react to what you can't see.

While newer installations on vessels may be capable of utilizing a centralized update cache onboard as described above, where the updates are pulled once and then deployed to multiple machines on the network, they are not common yet. The existing manual process should be used at a higher frequency on older vessels in the interim. Ideally this update process will synchronize with the scanning process, monthly for instance. The increased labor involved in cyber security management impacts the operational costs of the vessel and should be factored into the overall cost of increasing network bandwidth and integrating networked critical systems onboard.

10. Improvement of Security Posture through Scanning

Question: Since commencement of vulnerability scanning, has the security posture of onboard systems improved?

Company Comment:

"From the day we started vulnerability scanning the security posture of systems onboard has been improved because now we can monitor all security risks and fix/remediate at the same time."

Expert Commentary:

Any process that increases visibility and awareness has the potential improve the hygiene of the devices and the whole network.

11. Identifying Intentional Tampering

Question: How do you view the risk of intentional/criminal tampering with existing data (by disgruntled crew members/employees for example). How do you identify and deal with these incidents?

Company Comment:

There is the possibility that company personnel, on board and ashore, could compromise cyber systems and data. In general, the company should be prepared that this may be unintentional and caused by human error when operating and managing IT and OT systems or failure to respect technical and procedural protection measures.

We have created a policy for unauthorized access for pc's/servers and data.

We have restricted user access for any crew member to pc and data access.

Production pc's/servers are backed up daily to a central storage system.

Vessel's important data are replicated live to Shore using dedicated software for replication.

Key operation data are stored in a secure database of onboard ERP system, crew only has restricted access to relevant data according to rank.

Expert Commentary:

The issue of intentional tampering by crew came up during the interviews we conducted during our cyber security survey for policy considerations.

In every case there had never been an incident to date. The vast majority of the critical systems are located in access restricted areas such as the bridge and engine room. Another area of concern is cabling, it is unclear to what extent vessels are protecting cabling that connects critical systems such as depth finders, helm control, cargo systems, radar etc. Ideally all critical communications lines should be run within a suitable conduit to prevent physical tampering.

As for malicious tampering by outsiders, most of the masters interviewed had either experienced an onboard ransomware attack or knew of a master who had

The data itself is often not backed up comprehensively onboard, but this is changing. The biggest challenge has been additional charges for the service to ship owners. In multiple cases the Master devised their own way to backup and restore data should the need arise.

12. Referencing the 5 Stages Recommended by BIMCO

Question: Please comment on the 5 stages recommended by BIMCO[3] as part of the National Institute of Standards and Technology (NIST) Cybersecurity Framework[4] (Identify, Protect, Detect, Respond, Recover) for cyber security.

Company Comment:

"BIMCO outlines an approach to cybersecurity that includes: Identify Threats, Identify Vulnerabilities, Assess Risk, Develop Protective and Detective Controls, Establish Contingency Plans, Respond and Recover from Incidents. This expands on the NIST's five."

To put this into more practical terms the steps at their most basic can be summarized as follows:

NIST	BIMCO	Examples
Identify	Identify Threats	Threat Intelligence Feeds Table Top Exercises
	Identify Vulnerabilities	Vulnerability Scanning
	Access Risks	Vulnerability Assessment Penetration Testing Risk Assessment
Protect	Develop Protective Controls	Firewalls, Endpoint Protections, File Encryption, Mobile Device Management (MD)
Detect	Develop Protective Controls	Intrusion Detection, Log Monitoring, Network Traffic Sensors, SIEM
Respond	Respond	Malware Recovery Tools, Live Malware Analysis
Recover	Recover	Reimaging Process, Restore for Backups, Confirm System Integrity

We need to identify threats that a vessel may be targeted. A vessel may be targeted from activists, criminals or terrorists. The biggest threat for the vessel is the crew members. Most of the time this relates to unawareness. A user may have an infected USB and just plug it in on a vessel pc, this will infect the pc. For the Identification of vulnerabilities, we are using vulnerability management software to identify application/operating system vulnerabilities. In addition, we are in direct contact with hardware vendors for firmware upgrades. Further, we have initiated penetration testing to the vessel to expose our vulnerability and security breaches.

Accountability and ownership for cyber security assessment should start at the senior management level of a company, instead of being immediately delegated to the ship security officer or the head of the IT department. We have created a Vessel IT Cyber security team responsible to educate crew and to strengthen Vessel Security and create policies. In addition, Risk Assessment Documentation has been created for every vessel To develop protection and detection measures we have taken the actions below:

- Enabled IPS (Intrusion Prevention) and IDS (Intrusion Detection) on Vessel Firewalls.
- Malicious Websites are blocked from the Firewall.
- Network Segregation has been applied to prevent unauthorized access from Crew PC's to Vessel PC's.
- Regularly change PC Passwords and Access Point Passwords.
- Antivirus Endpoint Protection has been applied to all Computers.
- Vulnerability Management Software.
- Threat Intelligence Software. We can have a clear view with Reports of what happens in the Vessel Network.

For the establish of contingency plans we have created risk assessment documentation which clarifies how the Captain must react to each threat. The local IT Department is always on call for security issues if required. In addition, our Antivirus provider is available to resolve any malware issue if advance assistance is required. With Threat Detection our supplier will provide remediate action to the crew if physical assistance is required.

To report a Cyber Security Incident, we take the following actions:

- Antivirus will export a report from the cloud portal.
- Threat Intelligence Platform will export on the same day a report for any threat/breach found in the network.

To Remediate a Cyber Security Incident, we take the following actions:

- Disconnect the infected pc from the network and format the pc.
- Remove computers from network and scan computers for any threats.
- Check Root cause analysis for the threat to check expandability of the threat.
- Request the assistance from our Antivirus partner to confirm that threat is removed and pc's are clean.
- Monitor computers for abnormal status**.**

Expert Commentary:

Many companies' cyber security programs focus more heavily on one or two aspects of security operations. Often the program has simply grown organically over time, more or less reacting to emerging threats as they arise. Over emphasis on protective controls for example. Protective controls always fail at some point so they must be offset by robust detective controls. Likewise, good controls are not enough to effectively manage an incident. When the "bad day" happens a well prepared and practiced incident management process will limit the cost and disruption of the incident. When evaluating your security program, it helps to engage outside expertise to offer other perspectives and objectively challenge internal assumptions. This can help identify blind spots and result in a more balanced and intelligently layered approach to managing cyber security risk.

13. Software Quality and Alternative Means of Communication

Question: Please give your view of the quality of the software used in IT & Operational Technology (OT) Systems, software security by design/default of IT & OT systems. Have you considered alternative means of maritime communication?

Company Comment:

There is a dedicated group in our company responsible for testing new software solutions before launching them live on a vessel. Software is tested on several PC models for performance, we are not implementing new software onboard vessels that could cause performance issues. WE will test software for any vulnerabilities or security risks, run a full scan and test for the new software to be sure that it is safe. The vendor has to confirm that every firmware update of hardware is sent to the vessel to avoid any vulnerability risks.
We have been using L-Band (FBB) and iridium IOP for many years. We are now in the stage of upgrading FBB plans to new VSAT KA and KU band. We are in discussions for the new iridium Certus.

Currently we are installing new VSAT systems with a load balancer with FBB or iridium. This will ensure that vessels will not have any loss of communication. In addition, we are testing 3g/4g Data Connection for the vessel from the shore with a range for more than 30KM at sea.

Expert Commentary:

Application development security processes for onboard software systems have arguably lagged behind shore-based software with a similar operational function. This stands to reason as these systems are more isolated and have not been exposed to remote attack as frequently in the past. It is also more difficult to update systems at sea. Some imbedded systems in use even utilize end-of-life and non-supported components including the operating systems. This is of course changing but many of the legacy systems remain in use. That is changing but with change comes both advantages and disadvantages. It's now a lot easier with higher network speeds available to update systems but the same availability is exposing systems to more threats and thus increasing risk.

In some cases, onboard systems are required to run old and vulnerable versions of web browsers and client-side java to function properly with legacy systems. This occurs less frequently on a shore-based infrastructure and will have to change as the Internet becomes more widely available onboard. When it is necessary to use outdated or unsupported software components compensating controls should be devised and deployed to offset risk. For example, if it is absolutely necessary to use an old version of a browser its communications can be restricted with a host-based firewall so that it can only communicate with the endpoint hosting the required application. An up to date browser could then be used for general Internet browsing. While compensating controls like this are not ideal it is important to understand that security measures often negatively impact usability. Finding the right balance of managing risk while maintaining usability requires careful consideration and in some cases some trial and error.

14. Documenting the Management Process

Question: What metrics do you use to track vulnerability state over time and document the management process?

Company Comment:

"For the Cyber Security Device onboard a report is exported daily and monthly."

"Based on that report we will find the fix that we need to apply and after we finish we will document in a report changes applied."

"The same applies for the remote vulnerability assessment."

Expert Commentary:

It's a good idea to track vulnerabilities over time at both the vessel and the enterprise level. This documents the effectiveness of the management process or highlights opportunities for improvement. The most dramatic improvement usually comes between the first and second scans as there is usually some low hanging fruit. Compiling a running 12-month histogram of total vulnerabilities in each severity level will succinctly depict the effectiveness of the vulnerability management product.

15. Third Party Assessments

Question: Do you or are you intending to use third party services? Which services are you looking to use? Entirely with current IT and communication dept. staff?

Company Comment:

"Yes, we intend to use and we are using third party services for Cyber Security for the Vessels, Vulnerability assessment and penetration testing."

Expert Commentary:

Having a third-party conduct or review your vulnerability scans or perform a more in-depth penetration test is always a good idea. Ideally a third party specializing in security will look at the subject environment through the eyes of an attacker rather than those of an auditor. This is very different from the typical IT perspective in that attackers are adept at leveraging multiple seemingly insignificant advantages, often acceptable risks, to achieve a larger goal of an unacceptable risk. A penetration test may start with something as simple as an email or a phone call and end up with the (simulated) attacker taking control of administrative functions on multiple critical systems.

When selecting a third-party partner seek out professionals with relevant experience and consider limiting the scope to realistic attack scenarios. For example, you might consider physical access to data processing equipment a lower priority given how rare it factors in at this point in time and instead focus on testing with simulated malware which is a more common occurrence.

You may also want to consider the confidentiality of your relationship with the vendor. While it is important for a vendor to provide references, a vendor that openly advertises their relationships with other parties can inadvertently put you at risk by proxy. Make sure your vendors understand the importance of secrecy so publicly available marketing information cannot form the basis of a future social engineering attack.

16. Financial Aspects – Is it Worth the Cost?

Question: Many ship owners and ship managers do not yet agree that investment is required in cyber security management. Please give your view?

Company comment:

"Years ago, price may have been the issue."

"After recent attacks at major global companies many owners are revising their IT and Security infrastructures and budgets. In addition, in accordance with future European/Shipping regulations Owners have to apply certain security procedures/software to their vessels."

Expert Commentary:

Technology can be used for cost reduction through efficiency gains. Technology in a business environment without a clearly defined and well understood return on investment is simply folly. Unfortunately, and all too often the efficiency gains are considered in implementation while the soft costs of managing increased risk are ignored, downplayed or only realized in retrospect after a costly incident. This can result in a technology being hastily deployed without considering the whole business process and then risk management cost is seen as unnecessary or added overhead. The two must be considered together to make rational decisions on what kind and how much technology to implement in any given circumstance.

17. Summary

As far a security process goes vulnerability management is good value. It's relatively inexpensive compared to protective and detective controls and leverages operational IT processes already in place. It also helps cultivate awareness of the networking environment and can help ship managers demonstrate a positive security posture onboard their vessels. It limits the effectiveness of malware by eliminating known vulnerabilities from the environment. It is especially damaging to a company's reputation when a major incident occurs based on a known vulnerability that should have been patched already.

There are vulnerability scanning products and services to suit every budget from sophisticated enterprise management tools like Tenable's Nessus[5] and Rapid 7's Nexpose[6] to stand alone open source initiatives like OpenVAS[7] and lots to choose from in between. Given the high impact and low cost there really isn't a good reason not to have a vulnerability management process in place.

18. Contributors

The Cyprus Shipping Chamber wishes to express its particular appreciation to the members of the Chamber's ICT Sub-Committee, Mr. Gideon Lenkey, Director Technology of EPSCO-Ra, Mr. Andrew Ioannou, Managing Director of EPSCO Cyprus Ltd and Mr. Elias Eliades, IT Officer of Bernhard Schulte Bernhard Schulte Shipmanagement (Cyprus) Ltd for their valuable contribution in preparing the Vulnerability Management Case Study. Appreciation is also extended to the rest of the members of the Chamber's ICT Sub-Committee for their input.

19. References

1)https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/

2) Common Vulnerabilities and Exposures - https://cve.mitre.org/

3) https://www.bimco.org/products/publications/free/cyber-secuirty

4) https://www.nist.gov/cyberframework

5) https://www.tenable.com/products/nessus/nessus-professional

6) https://www.rapid7.com/products/nexpose

7) http://www.openvas.org/