NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
July 2019 (edition 2019-7)

This **electronic** publication is intended to inform port stakeholders about cyber security issues and provide information useful to safeguard seaport systems that may be vulnerable to cyber-attacks. The information contained herein is suitable for general release and members of the Northern California Area Maritime Security Committee are encouraged to pass it on to members of our maritime community. This news letter will be e-mailed to members of the Northern California Area Maritime Security Committee and posted on the Coast Guard's HOMEPORT portal within the Sector San Francisco port area.

IF YOU SEE SOMETHING, SAY SOMETHING

To report a crime in progress, call 911 or your local police department. To report maritime related suspicious activities or breaches of security call the National Response Center (NRC) at 800-424-8802 or a cyber-attack to the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870. After calling the NRC or NCCIC call the Captain of the Port, San Francisco, at 415-399-3530.

TABLE OF CONTENTS

ARTICLE SUMMARIES

- **To Air-Gap or Not to Air-Gap** – a discussion about air-gapping IT network.
- **Maritime Cyber Training Website** – informational article about a website.
- **10 Steps to Maritime Cyber Security** – a discussion about cybersecurity management.
- **California Cybersecurity Integration Center** – information about Cal-CSIC.

MAIN ARTICLES

To Air-Gap or Not air-Gap Industrial Control networks, by Gary DeFazio (ICS Security), 17JUN19

What is air gapping, and why do we air-gap networks? What camp are you in? In the camp that believes in air-gaps, or the other set that says they truly do not exist?

Air-gap networks are networks that are physically and logically isolated from other networks where communication between these networks is not physically or logically possible. Over the years, many networks in many different verticals from governments, military, financial services, nuclear power plants and industrial manufacturing, to name a few, have been so-called "air-gapped."

In the industrial vertical, these air-gapped networks were the networks that supported the industrial control systems within the plant or factory where communication was physically or logically isolated between the plant and the enterprise networks.
In today's Industry 4.0 revolution where the network is the control system, analyzing data from the industrial process is key to drive optimization and efficiency, and where more and more field devices are "smart" (connected and managed through the network), is the notion of air-gapped industrial networks practical for the future or is there really an air-gapped network today?

Is it effective? False sense of security?
In theory, air-gapped networks seem like a good idea. In practice, that is another story.
Do they really guarantee isolation from the Internet or from the corporate business network? It has been proved in a number of different scenarios that air-gapped networks can be infiltrated. The most famous of these examples is Stuxnet, the worm that was able to target and disrupt the process of enriching uranium that could be used to manufacture nuclear warheads in Iran's Natanz nuclear facility.

There are many other non-threatening examples like modems and wireless networks being set up by contractors, maintenance, or control engineers to make their lives easier to transfer data in or out of the air-gapped networks. What about transient devices such as laptops, tablets and smart phones? Do not forget about removable media (USB, CDROM, etc.), remote access and data coming via SNEAKERNET (any means of transferring data without it traversing a network). Are these environments truly air-gapped?

All of these examples prove that nothing is truly air-gapped or that it cannot stay 100% air-gapped over time. Do air-gaps give us a false sense of security? How many times do cybersecurity professionals hear, "Oh, we are air-gapped. We do not need to worry about cyber security"? If that is the case, how does someone know if they are air-gapped if they do not assess or monitor their networks for
1) new data coming in from removable media/transient devices or
2) external network connections being set up with modems or VPN's.

At the end of the day, new data is coming into these so-called "air-gapped" environments. How do we manage it?

The Million Dollar Question

How do you know? How do you know if data is coming in or going out of your network? How do you know if there are external connections being set up for ease of use for employees, contractors or vendors?

To be able to answer the variety of "how do you know" questions, it comes down to knowing your network and placing preventative controls around it to be able to continuously answer questions like these:

- What devices are on it?
- What are those devices communicating?
- Who are those devices communicating to?
- What is normal communication between those devices?
- Are any external connections being set up?

Just like we monitor and measure quality characteristics of the output of our industrial processes (i.e. inventory, scrap, rework, physical dimensions, overall equipment effectiveness, accidents, etc.), we need to monitor and measure our environments for abnormal behavior – configuration changes, communication pattern changes, exploitation of vulnerabilities and new or unexpected network connections, etc. – which will help us recover from special causes that impact the operation of our process including but not limited to misconfiguration, human error, cybersecurity events, machine failure, etc.

Where do you start?

If you have not started your industrial cybersecurity journey, a good place to start is with an industrial cybersecurity vulnerability or risk assessment.

Cybersecurity vulnerability assessments typically find that an environment is never completely air-gapped. Assessments usually find evidence of unsanctioned external connections created by control engineers, most often for non-threatening, non-malicious reasons.

These undocumented, unapproved network connections are usually created to ease an engineer's system maintenance and/or troubleshooting responsibilities to avoid from having to SNEAKERNET a file or program to the control environment. Most of the time, these are only set up to provide short term relief, but what happens is that connections forget to be torn down, leaving the air-gapped network wide open to other communication channels where behavior tends to lend itself to the malicious kind.

Tripwire's professional services team performs cybersecurity vulnerably assessments and will review your environment for weaknesses that could impact your industrial process and make remediation recommendations. One of the areas we will review is if you have any external network connections where data could be coming in or going out of your environment. For more information, check have a look here.

What else do you need to do?
Concentrate on foundational cybersecurity controls. Do not try and boil the ocean with advanced techniques. Three key foundational cybersecurity controls that will mitigate the most risk from both internal and external threats are the following:

1. Understand and manage data flows, aka network communication.
    - Maintain an accurate asset inventory (vendor, make, model, firmware version, etc.)
    - Monitor device data flows, what is expected and what is abnormal.
2. Enforce expected communication patterns or data flows with network segmentation
3. Monitor and manage configuration changes of all devices within the control network

With regards to managing data flows, it all starts with creating and maintaining an accurate asset inventory inclusive of hardware and software. Once an accurate asset inventory is complete, you can then begin to understand and manage all data flows (communication patterns) in and out of your control networks for things like:

1. File transfers – FTP, SFTP/SCP, etc.
2. Transient devices – laptops, tablets, mobile phones, etc.
3. Removable media – i.e. USB keys
4. Internal network connections – intra cell or zone as well as inter cell or zone
5. External connections – all connections to/from business or corporate network, suppliers, vendors, etc.
6. Wireless networks – especially those set up on the fly for ease of use.

How you gain visibility to data flows?
You must know what is connected to your network (accurate asset inventory) and then monitor data flows from those devices traversing your network.

Tripwire offers a passive monitoring solution, Tripwire Industrial Visibility, that has been developed from the ground up to understand industrial protocols and industrial control networks, to inventory devices, (vendor, make, model, firmware version, etc.) as well as understand what protocols devices are using to communicate on the network. Tripwire Industrial Visibility has a learning mode where all assets and communication baselines are learned, and then once the solution is placed in operational mode, it will alert on any devices from those operational baselines.

Once data flows are learned and understood, the next step is to put a preventative control in place to enforce those communication patterns. This is where an industrial security appliance such as the Tofino Xenon plays. It is able to perform deep packet inspection and sanity checking on the industrial protocol to enforce authorized communication between devices and/or networks. This appliance helps implement the zones and conduit approach outlined in IEC 62443 where zones are defined as assets of a similar function/risk model (aka HMI zone or PLC zone) and conduits outline the authorized or expected communication between devices in one zone to another zone (aka only allow Modbus TCP between HMI zone and PLC zone or only allow DNP3 between the substation zone and the control center zone). This is a recommended

approach whether you have an air-gapped network or not, as it mitigates risk of propagation of malicious or unexpected traffic traversing east/west within the factory or plant floor.

Last but certainly not least is the ability to manage changes to device configurations. This includes all kinds of devices such as controllers, HMI's, RTU's, engineering workstations, routers, switches, databases and firewalls.

What happens a lot of times when there is a production outage that is impacting the plant's ability to make product? The result of this is that something changed – a configuration setting, firmware version, new port opened, new device connected to the network, etc. How long does it take to first understand something changed and then to revert that change back so that the process is back to operating at a functional, productive state?

Managing changes and understanding if changes adhere to authorized work orders in ticketing systems is the core competency of Tripwire Enterprise. Tripwire Industrial Visibility can also be used to manage changes, particularly around changes in controllers, whether it be new ladder logic added to a program or whether it be a change to the controllers operating mode: run, program, test, etc. Don't let changes manage your day-to-day operation. Manage changes through visibility so that a change management policy can be enforced.

Air-gap or not – Visibility, Preventative Controls and Continuous Monitoring are key behaviors Monitoring solutions are needed irrespective of whether you air-gap to maintain full control of your industrial environment. Tripwire solutions can help provide visibility, protective controls and continuous monitoring to help provide visibility to and protection from cyber events that threaten safety, productivity and quality. Check out a prior blog to learn more.

Maritime Cyber Training Website, Paul Martin, 21JUN2019

Site: Maritime Cyber Security Guidance, Useful Documents, Articles & Publications for Students; **https://www.maritimecybertraining.online/page/library**

According to their website: "Here you will find a library of useful resources including maritime and offshore industry cyber security best practice guidelines, cyber risk assessment advice and a suite of the latest information, that can be used to help you through your studies or for continued professional development. Please feel free to read them online or click and download them for offline use."

Looking through the available documents I found the following examples:

- Various ABS documents/reports
- Various DNV documents/reports
- Various BIMCO documents/reports
- Various Hewlett-Packard documents/reports
- Code of Practice for Cybersecurity for Ships
- IET Code of Practice for Cybersecurity for Ports and Port Systems

10 Steps to Maritime Cyber Security, Safety4Sea, 21MAR2018

A guide to manage cyber risk (**https://safety4sea.com/10-steps-to-maritime-cyber-security/**)
Ships are increasingly using systems that rely on digitization, integration, and automation. As a result, security of data and other sensitive information has become a major concern of maritime. Training and awareness of appropriate company policies and procedures may provide an effective response to cyber incidents. Here are some guidelines to help maintain maritime cyber security.

Maritime Cyber Security Step 1: Network security
Nowadays, networks are critical to the operation of a ship. It is imperative that these systems do not expose systems to cyber-attack. However, shipboard computer networks usually lack boundary protection measures and segmentation of networks. Such networks are among the most common cyber vulnerabilities on board existing ships, according to a paper published by the International Chamber of Shipping. Simple policies implementation and appropriate architectural and technical response can help manage and/or prevent these attacks from causing harm to your organization. Onboard networks should be partitioned by firewalls to create safe zones. The fewer communications links and devices in a zone, the more secure the systems and data will be.

Maritime Cyber Security Step 2: Malware prevention
Malware is any malicious content which is designed to access, gain control and damage systems. In other words, a malware could seriously impact your ship's systems or services. Organizations should implement an appropriate anti-malware policy to defend in depth their networks both onboard and ashore, filter out unauthorized access and malicious content.

Maritime Cyber Security Step 3: Risk Management Regime
Why to embed an appropriate risk management regime across a shipping organization? Organizations should clearly communicate their approach to risk management with the development of applicable policies and practices. These aim to maintain marine cyber security, ensuring that personnel onboard and ashore is aware of the approach, how decisions are made, and any applicable risk boundaries.

Maritime Cyber Security Step 4: Secure configuration
Configuration management improves the security of systems and eliminates the risk of compromise of both them and any information. Therefore, organizations should develop a strategy to remove unnecessary functionality from systems, and quickly fix known vulnerabilities!

Maritime Cyber Security Step 5: Managing user privileges
All users should be provided with a reasonable level of system privileges and rights needed for each role. The granting of highly elevated system privileges should be carefully controlled and managed; this principle is sometimes referred to as 'least privilege'.

Maritime Cyber Security Step 6: Employees education and awareness
Personnel both onboard and ashore play a critical role in a shipping organization's security and so it's important that security rules and the technology provided enable them to do their job. A

systematic delivery of awareness programmers and training always deliver security expertise as well as help establish a security-conscious culture within the organization.

Maritime Cyber Security Step 7: Incident management
It is of high importance that an organization identifies any internal or external source of specialist incident management expertise. Effective incident management policies and processes may help to improve resilience and reduce any impact with respect to maritime cyber security.

Maritime Cyber Security Step 8: Monitoring
Good monitoring is the answer to the question "How do I detect actual or attempted attacks on systems and services?". Monitoring allows organizations to ensure that systems are being used appropriately, complying with any regulatory requirement.

Maritime Cyber Security Step 9: Removable media controls
Wondering why to produce removable media policies? These can control the use of removable media for the import and export of information, limit the types of media that can be used together with the users, systems, and types of information that can be transferred.

Maritime Cyber Security Step 10: Remote system access
Remote system access not only offers great benefits, but it also exposes new risks. Risk based policies and procedures should be established in order to support remote access to systems, applicable to service providers.
Either way, cyber incidents can put both organization's operations and human lives at risk. One thing is sure, operators will not be able to defend themselves alone! Like in many other digital developments, experts suggest cooperation and collaboration and resilience to find the right answers when it comes to maritime cyber security.

California Cybersecurity Integration Center, Paul Martin, 21 JUN 2019

From the website: On 31 August 2015, the Governor of California signed Executive Order B-34-15, creating the California Cybersecurity Integration Center (Cal-CSIC) with the responsibility to:

1. Reduce the likelihood and severity of cyber-attacks;
2. Improve inter-agency and cross-sector information coordination;
3. Prioritize cyber threats and alert potential victim entities; and,
4. Strengthen the state's cybersecurity strategy.

The Cal-CSIC is made up of four core partners, the California Governor's Office of Emergency Services, the California Department of Technology, the California Military Department, and the California Highway Patrol.

HOW YOU CAN HELP PROTECT CALIFORNIA
State, local, and tribal governments, non-governmental organizations and the private sector can partner with the Cal-CSIC by registering to receive Alerts and Advisories, sharing IOCs and cyber incident reports, and connecting to the California Automated Indicator Exchange.

- Register online to receive cybersecurity threat information for your organization at https://calcsic.org.

- Email the Cal-CSIC to learn more about sharing of IOCs and connecting to the California Automated Indicator Exchange at calcsic@caloes.ca.gov.

- Report cyber incidents to the Cal-CSIC at (833) REPORT-1 or calcsic@caloes.ca.gov.

FBI Warns Users to Be Wary of Phishing Sites Abusing HTTPS, John Dunn, 12JUN19

HTTPS signifies an encrypted, secure connection with a server, but doesn't signify that the server is legitimate. The FBI recently issued a warning that too many web users view the padlock symbol and the 'S' on the end of HTTP as a guarantee that a site is trustworthy. Given how easy it is to get hold of a valid TLS certificate, as well as the possibility that a legitimate site has been hijacked, this assumption has become dangerous. Not having an HTTPS site has become a negative. In 2018, Google's Chrome and many other big-name browsers including Firefox and Edge began marking non-HTTPS sites as 'not secure' in the address bar. Soon, website owners and web users got the message that HTTPS was good and the lack of it was bad. However, criminals caught on quickly, which explains the surge of phishing sites that started using HTTPS in their domains around 2017. The worry now is that attackers are moving beyond this crude ruse and are on to abusing domains backed by legitimate certificates. Security company AppRiver recently documented how attackers have started abusing Microsoft Azure's Custom Domain Name registrations to host what are, in effect, fully credentialed phishing sites. HTTPS is good because it secures traffic from prying eyes; however, as with the related problem of rogue VPNs, the presence of an encrypted connection should not be understood as a security guarantee on its own. Beyond not blindly trusting HTTPS domains, the FBI recommends checking for misspellings in domain names. Additionally, users should use a desktop password manager, which checks the validity of domains before offering to autofill credentials. If it doesn't present credentials, that could be a giveaway that something isn't right about a site.

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan **must report** cybersecurity suspicious activities or breaches of security to the Coast Guard's **National Response Center (NRC)**:

- Phone 1-800-424-8802 or direct phone line at 202-372-2428
- Fax 202-372-2920
- Web: http://www.nrc.uscg.mil/

After calling the NRC, call the Captain of the Port, San Francisco, at 415-399-3530.

The Federal Bureau of Investigation (FBI) should be notified of cyber security breaches:

- FBI Headquarters – threats and crime reporting: https://tips.fbi.gov/
- San Francisco Office – 415-553-7400 (san.francisco@ic.fbi.gov)
- Sacramento Office – 916-841-9110 (http://www.fbi.gov/sacramento)
- Internet Crime Center – http://www.ic3.gov/complaint/default.aspx
- IngraGard Website – https://www.infragard.org/

U.S. COAST GUARD HOMEPORT PORTAL

The U.S. Coast Guard maintains links to various sources of maritime security information on its HOMEPORT information portal. The link to U.S. Coast Guard's HOMEPORT maritime security information portal is:

- Web – http://www.homeport.uscg.mil/

- Report cyber incidents to the Cal-CSIC at (833) REPORT-1 or calcsic@caloes.ca.gov.

CUSTOMER FEEDBACK

How are we doing? Please send feedback about this newsletter to Mr. Paul Martin, USCG Sector San Francisco, at:

- E-mail – Paul.R.Martin@uscg.mil

Note: articles appearing in this newsletter were submitted by port stakeholders and posted without editing. If you have an article to post, please provide the article to Mr. Martin at the above e-mail address. This newsletter is a quarterly publication and generally published shortly before a meeting of the Northern California Area Maritime Security Committee. **This newsletter is for public information purposes only**; articles containing proprietary, sensitive but unclassified, or classified information will not be accepted. The U.S. Coast Guard reserves the right to decide which articles are published in this newsletter.