Port of Vancouver USA

Port of Vancouver USA

Cybersecurity Workshop

Commission meeting

SEPTEMBER 13, 2022

CHRIS CARTER, INFORMATION SECURITY ANALYST

Introduction

Internal Controls

Internal Controls

- Information Security Committee.
- Internally working together.
- Layered Anti-virus approach.
- 100% Multifactor authentication.
- USCG NVIC Cybersecurity Annex.
- Robust logging and correlation.
- Backups.
- Vulnerability Management.
- Critical Insight - 24/7.

Pandemic

Pandemic

- Adoption to cloud already in process.
- Perimeter was gone.
- Disaster Recovery and Business Continuity plan just completed.
- Didn’t miss a beat.
- Education.

Information Sharing

Information Sharing

- 5 years participation in information sharing.
- Immediate successes.
- February 2020 – Founding board member of the MTS-ISAC.
- Chair quarterly Microsoft 365 Working group.
- Established Regional information sharing network.

Maritime Information Exchange

Weekly cyber tips

- Tip of the week.
- Phishing emails seen.
- What to expect to see.
- News impacting you or your family.
- Maritime/Port specific cybersecurity.
- Upcoming training/ webinars.

Cybersecurity Tips for the Week – Aug 9th 2021

Tip of the Week

For this week, some travel tips from the FBI Portland office tech Tuesday blog.

- Leave any devices you don't truly need at home.
- For those devices you do take, make sure to update all anti-virus and malware options before departing and again after returning home.
- Also, before you travel, make sure to change your passwords and PINs to new, strong options that you do not use at home. When you get back after your trip, change them again to another new option.
- Make a backup of your device in case your phone or laptop gets hacked or targeted in a ransomware attack. Remember—back-ups should always be kept offline so the bad guy can't access those as well.
- Make sure your wireless and Bluetooth auto-connect and remote-connect settings are off while traveling. They are handy to use when at home, but on the road you could accidentally connect to a malicious network without even knowing it.
- Likewise, it's tempting to take advantage of free WiFi options when in airports, hotels, coffee shops, and elsewhere—but be careful. If you can get in, so can a hacker. If you must connect to a public network, make sure to only use "https" sites. Also remember—never do shopping, banking, or access sensitive data—such as your health care portal—while on a public network.
- Using your own data network connection or using a VPN are always better options.

https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-against-travel-tech-fails

Phishing Report (Subjects of phishing emails seen)

- **Fake fax/ Voicemail messages are being seen across the country in the Maritime community. This continues this week with a very high volume.**
- Executive spoofing emails (Continue)– Usually ask for a task with urgency.
- Display name spoofing imitating several companies and/ or associations.
- Domain names with one to two letters off. Seeing a lot of this targeting the energy sector.
- Fake Invoices for Norton/ McAfee Security 360 Plan.
- Spoofed display name emails from the "IT Department" or "Support Department".
- Fake Office 365 phishing emails with subjects as "Account expired", "Messages is quarantine" or "Verify Your Mail {"Your name"} To Avoid Deactivation" or anything warning you something is about to "Expire".
-

Tide Table – (What I expect to see this week)

- **Known contacts continue to get compromised.**
- Fake Office 365 messages. Password Expiration Notices seem to be popular.
- Spam calls and text messages.

Partnerships

Partnerships

- American Association of Port Authorities (AAPA).
- Washington Public Ports Association (WPPA).
- Columbia River Steamship Operators Association (CRSOA)
- Pacific Northwest Waterways Association (PNWA)
- Fusion Centers.
- InfraGard.
- Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC).
- Multi State Information Sharing and Analysis Center (MS-ISAC).
- United States Coast Guard.

“Firewalls”

125+ Deployed "Firewalls"

- What do I mean by "firewalls"?
- 11,000+ **reported** phishing emails over that last two years!
- **People**, Process, Technology.
- Rapid change.


THE MOST DANGEROUS PHRASE IN THE LANGUAGE IS, 'WE'VE ALWAYS DONE IT THIS WAY."
Rear Admiral Grace Hopper
WIKIMEDIA COMMONS/US NAVY - JAMES S. DAVIS
attn:

What's next?

What's next

- Adapt.
- Email Security.
- Revamp Cybersecurity training.
- Information sharing.

Thank You

Chris Carter
Information Security Analyst
Chris.Carter@portvanusa.com
360-693-3611