IMT 559 Final Project

Port of Seattle POAM

Binisha K, Dominic M, Vanshika S, Habib N

5/31/2024

For our final project we are sharing a comprehensive cybersecurity policy and Plan of Action and Milestones (POAM) for the Seattle-Tacoma Maritime Port, based on the NIST Cybersecurity Framework (CSF) 2.0. Our focus will be on mitigating threats posed by Volt Typhoon, a sophisticated offensive nation-state cyber actor based out of China. We will delve into three critical mitigation strategies from the NIST CSF 2.0 framework: Asset Management, Access Control, and Incident Response.

Volt Typhoon

Volt Typhoon is a nation-state cyber actor known for its sophisticated and targeted cyber-attacks on critical infrastructure. Volt Typhoon historical focus has been on collecting and exfiltrating sensitive information by compromising internet-connected devices related to critical infrastructure systems of Western states. This group employs a range of tactics, techniques, and procedures (TTPs) to infiltrate, persist, and exfiltrate sensitive information from their targets. Some key TTPs associated with Volt Typhoon include:

- Living off the Land techniques
- Phishing and Social Engineering: Using deceptive emails and messages to gain initial access.
    - Spear phishing Attachment -T1556
- Exploitation of Vulnerabilities: Leveraging known and zero-day vulnerabilities in software and hardware.
    - Exploits of Public-Facing Applications – T1190
- Credential Dumping and Lateral Movement: Obtaining and using stolen credentials to move laterally within a network.
- Data Exfiltration: Stealing sensitive information and transmitting it to external servers.
    - Data Staged – T1074

Volt Typhoon's activities pose significant risks to organizations, especially those managing critical infrastructure like ports.

Seatle-Tacoma Maritime Ports

The Port of Seattle is a vital hub for maritime trade and transportation, serving as a gateway for goods and services entering and leaving the Pacific Northwest. The combined Seattle-Tacoma Port is the 4th largest port in the United States. It encompasses various facilities, including shipping terminals, airports, and other transportation infrastructure, generating $12.4 billion in revenue and supporting more than 58,000 jobs in shipping, logistics, and manufacturing industries. The Port's operations are heavily reliant on information systems for logistics, security, and management functions. Given its strategic importance and interconnectedness, the Port of Seattle is a prime target for cyber-attacks from nation-state actors like Volt Typhoon.

Cybersecurity Policy for the Port of Seattle

1. Introduction

The Port of Seattle is committed to protecting its information systems and data from cyber threats and improving the cybersecurity posture. This policy outlines the framework and strategies employed to secure the Port's digital infrastructure against cyber-attacks, particularly from sophisticated nation-state actors like Volt Typhoon.

2. Scope

This policy applies to all employees, contractors, and third-party vendors with access to the Port of Seattle's information systems. It will also include all IT and OT systems, including port management systems, logistics, and operational technologies.

3. Objectives

- Protect the confidentiality, integrity, and availability of the Port's information systems and critical assets
- Implement strong security measures to prevent unauthorized access and protect against threat actors
- Develop an effective incident response plan to mitigate impact of an attack
- Ensure compliance with relevant regulations and standards including NIST 2.0 and IAPH
- Implement a robust recovery plan to ensure continuity after a threat event
- Promote a culture of cybersecurity awareness and responsibility with regular training

4. Responsibilities

- CIO/CSO: Overall responsibility for the cybersecurity program.
- IT Department: Implementation and management of technical controls. Responsible for incident response.
- Public Relations: Formulates public response plan as needed.
- All Employees and contractors: Adherence to cybersecurity policies and reporting of suspicious activities.

Selected Controls from NIST CSF 2.0

Control 1: Asset Management (ID.AM)

Policy Statement: The Port of Seattle will maintain an up-to-date inventory of all information systems, hardware, software, and data assets to ensure proper protection and management. Ensuring that all assets are securely sourced and remain securely operated is essential for fortifying the port.

Implementation Steps:

1. ID.AM-01: Conduct a comprehensive inventory of all IT assets.
2. ID.AM-02: Maintain inventories of hardware, software and systems managed by the organization.
3. ID.AM-03: Maintain cyber representations of the organization's authorized network communication and internal and external network data flows.
4. ID.AM-04: Maintain inventories of services provided by vendors and suppliers.
5. ID.AM-05: Prioritize assets based on classification, criticality, sensitivity resources, and impact on the mission.
6. ID.AM-07: Maintain inventories of data and corresponding metadata for designated data types.
7. ID.AM-08: Manage systems, hardware, software, services, and data throughout their life cycles
8. ID.AM-09 Implement automated tools for continuous monitoring and updating of the asset inventory.

Milestones:

- Month 1-3: Complete initial inventory of hardware, software, services, and systems.
- Month 4: Document network communication and data flows.
- Month 5: Inventory services provided by suppliers.
- Month 6: Classify and prioritize assets.

- Month 7: Inventory data and corresponding metadata.
- Month 8-9: Implement automation tools
- Ongoing: Manage assets throughout their life cycles.

Control 2: Access Control (PR.AA, PR.AT)

Policy Statement: Access to the Port of Seattle's information systems will be restricted to authorized users, processes, and devices, and will be managed through identity and access management (IAM) systems.

Implementation Steps:

1. PR.AA-01: Manage identities and credentials for authorized users, services, and hardware.
2. PR.AA-02: Proof identities and bind them to credentials based on the context of interactions.
3. PR.AA-03: Authenticate users, services, and hardware.
4. PR.AA-04: Protect, convey, and verify identity assertions.
5. PR.AA-05: Define, manage, enforce, and review access permissions, entitlements, and authorizations, incorporating principles of least privilege and separation of duties.
6. PR.AA-06: Manage, monitor, and enforce physical access to assets commensurate with risk.
7. PR.AT-01: Train all employees to be aware of cybersecurity risks with their relevant tools
8. PR.AT- 02: Provide employees with specialized roles with training and knowledge to perform relevant tasks with cybersecurity risks in mind

Milestones:

- Month 1-2: Manage identities and credentials.
- Month 3: Proof identities and bind to credentials.
- Month 4-6: Implement authentication measures.
- Month 7-9: Protect and verify identity assertions.
- Month 10-12: Define and review access permissions, entitlements, and authorizations.
- Ongoing: Manage, monitor, and enforce physical access controls.

Control 3: Incident Response (RS.MA, RS.CO, RS.IM)

Policy Statement: The Port of Seattle will develop and maintain an incident response plan to quickly detect, respond to, and recover from cybersecurity incidents.

Implementation Steps:

1. RS.MA-01: Execute the incident response plan in coordination with relevant third parties once an incident is declared.
2. RS.MA-02: Triage and validate incident reports.
3. RS.MA-03: Categorize and prioritize incidents.
4. RS.MA-04: Escalate or elevate incidents as needed.
5. RS.MA-05: Apply criteria for initiating incident recovery.
6. RS.IM-01: Update the response plan with lessons learned
7. RS.IM-02: Update response strategies

Milestones:

- Month 1-2: Draft and approve the incident response plan.
- Month 3: Establish coordination protocols with relevant third parties.
- Month 4-6: Conduct triage and validation training for incident reports.
- Month 7-9: Develop procedures for categorizing and prioritizing incidents.
- Month 10-12: Implement escalation and elevation procedures.
- Ongoing: Apply incident recovery criteria as needed.

Plan of Action and Milestones (POAM)

Control	Action Item	Responsible Party	Start Date	End Date	Status
ID.AM-01	Complete initial inventory of hardware, software, services, and systems	IT Department	06/01/2024	6/30/2024	Not Started
ID.AM-03	Document network communication and data flows	IT Department	09/01/2024	09/30/2024	Not Started
ID.AM-04	Inventory services provided by suppliers	IT Department	10/01/2024	10/31/2024	Not Started
ID.AM-05	Classify and prioritize assets	IT Department	11/01/2024	11/30/2024	Not Started
ID.AM-06	Inventory data and corresponding metadata	IT Department	12/01/2024	12/31/2024	Not Started
ID.AM-07	Manage assets throughout their life cycles	IT Department	Ongoing	Ongoing	Not Started

ID.AM-08	Classify assets and identify critical systems	IT Department	08/01/2024	08/31/2024	Not Started
ID.AM-09	Automated tools for continuous monitoring	IT Department	09/01/2024	10/31/2024	Not Started
PR.AA-01	Manage identities and credentials	IT Department	06/01/2024	07/31/2024	Not Started
PR.AA-02	Proof identities and bind to credentials	IT Department	08/01/2024	08/31/2024	Not Started
PR.AA-03	Implement authentication measures	IT Department	09/01/2024	11/30/2024	Not Started
PR.AA-04	Protect and verify identity assertions	IT Department	12/01/2024	01/31/2025	Not Started
PR.AA-05	Define and review access permissions	IT Department	02/01/2025	03/31/2025	Not Started
PR.AA-06	Manage, monitor, and enforce physical access	Security Team	06/01/2024	Ongoing	Not Started
PR.AT-01	Cybersecurity training	IT Department	07/01/2024	Bi-annual	Not Started
PT.AT-02	Specialized training for relevant teams	IT Department	07/01/2024	Bi-annual	Not Started
RS.MA-01	Draft and approve incident response plan	Incident Response Team	06/01/2024	07/31/2024	Not Started
RS.MA-01	Establish coordination protocols	Incident Response Team	08/01/2024	08/31/2024	Not Started
RS.MA-02	Conduct triage and validation training	Incident Response Team	09/01/2024	11/30/2024	Not Started
RS.MA-03	Develop categorization and prioritization procedures	Incident Response Team	12/01/2024	01/31/2025	Not Started
RS.MA-04	Implement escalation and elevation procedures	Incident Response Team	02/01/2025	03/31/2025	Not Started
RS.MA-05	Apply incident recovery criteria	Security Team	Ongoing	Ongoing	Not Started

RS.IM-01	Update the response plan	IT Department	Ongoing	Quarterly	Not Started
RS.IM-02	Update the response strategy	IT Department	Ongoing	Quarterly	Not Started

Conclusion

The implementation of this cybersecurity policy and POAM will enhance the Port of Seattle's ability to protect its information systems against cyber threats from sophisticated nation-state actors like Volt Typhoon. Regular reviews and updates to this plan will ensure its effectiveness and relevance in an evolving threat landscape.