DEPARTMENT OF VETERAN AFFAIRS (VA)
VETERANS HEALTH ADMINISTRATION (VHA)

The Threat Environment and Current Agency Snapshot

Presentation for: Federal Facilities Council, Operational Technology and Control System Security for Federal Facilities

Presented by: Nathan Hizer P.E., Office of Healthcare Engineering
Date 7/9/2024

The Threat Environment and Current Agency Snapshot

Situation, Challenges and What Are We Doing!

- Visibility
  - Inventory
  - Vulnerability Management
  - Onboarding Software
  - Security Controls- Authority to Operate (ATO)
  - Moving to cloud-based system- FEDRamp Approval
- Detection
  - Threat Detection
  - Anomaly Detection
  - Root Cause Analysis
- Response
  - Forensics Tools
  - Playbooks

Inventory

- Public Law 116-207 (12/4/2020)- Internet of Things Cybersecurity Improvement Act of 2020
  - To establish minimum security standards for Internet of Things devices owned or controlled by the Federal Government, and for other purposes.
  - Requires NIST and OMB to take specified steps to increase cybersecurity for Internet of Things (IoT) devices.
  - NIST Required to develop and publish standards and guidelines for federal agencies
    - **NIST Special Publication 800-82 R3 (9/2023)** Guide to Operational Technology (OT) Security (Previously Industrial Control Systems (ICS) Security)
    - **NIST Special Publication 800-213 (11/2021**)- IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements
  - GAO to report to Congress on IoT efforts
    - **GAO Audit in progress**
  - OMB to review agency information security policies and principals basis of the NIST standards.
    - **Current data call M-24-04**: **Due 9/30/24**

Inventory

- OMB M-24-04: FY24 Guidance on Federal Information Security and Privacy Management Requirements
  - Section I: Increasing Coordination with and Visibility of Continuous Diagnostics and Mitigation Capabilities
  - **Section II: Internet of Things**
  - Section III: Requirements for FISMA Reporting to OMB and DHS
  - Section IV: CIO Reporting
  - Section V: IG Reporting- Annual IG Reporting
  - Section VI: SAOP Reporting- Privacy Reporting Item
  - Section VII: Agency Head Letter for Annual Reporting Requirement to OMB
  - Section VIII: Annual Reporting to Congress and Government Accountability Office
  - Section IX: Incident Reporting Requirements

Inventory

- What to Inventory- Definition of IoT Device
  - NIST defines IoT devices as those that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. Many IoT devices constitute operational technology (OT), defined by NIST as "[p]rogrammable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.
- Other Names Internet of Things (IoT)
  - Operational Technology (OT)
  - Special Purpose Systems
  - Industrial Internet of Things (IIoT)
  - Industrial Control Systems (ICS)
  - Building Automation Systems (BAS)
  - Energy Management Systems (EMS)
    - Supervisory Control and Data Acquisition Systems (SCADA)
    - PLC (Programable Logic Controllers)
    - Distributed Control System (DCS)
    - Intelligent Electronic Devices (IED)
    - Physical Access Control Systems (PACS)

Inventory

What VA Systems are Included as IoT:

- Building Automation Systems
- Temperature Monitoring Systems
- Physical Access Control Systems (PACS)- Controls the electronic access systems, intrusion detection
- Camera monitoring systems (CCTV)
- Power Monitoring/SCADA- Controls the electrical systems (Utility, emergency generators, uninterruptable power monitoring (UPS) etc.
- Energy Management Systems/Utility Metering- Controls monitoring various utility systems such as electrical, water, natural gas, steam and chilled water.
- Fire Alarm Systems- Fire detection, alarm and mass notification systems
- Lighting Control Systems- Controls interior and exterior lighting systems
- Vertical Transportation Systems- Elevators and Escalators (Video, texting and 2-way voice communications)
- Emergency Management Systems-Mass Notification to staff, patients and visitors
- Laundry Plant Controls

Inventory

- Paging/2-Way Radios-On Site Communication Systems
- Wander/Elopement Alarm Systems- Patient wander alerting systems
- Nurse Call-Bed Site patient communication equipment
- Medical Gas Alarm System (Air/Oxygen/Vacuum/Nitrogen)- Medical gas alarm systems
- Pneumatic Tube Systems-Transportation systems for various items around a facility.
- Video Boards-Messaging Systems at front gate and in waiting rooms (SmartTV's)
- Water System (Purification/RO/Steam/Distilling/Irrigation)
- Work Order Management Systems
- Autonomous Systems (Laser Guided Vehicles (LGV), Robotic vehicles)
- Smart Vehicles (Most vehicles)
- Police Equipment-(Vehicle mounted cameras, body cameras, testing equipment)
- Fuel Management and Alarms
- Queuing systems (Now Serving)
- Testing Devices (Power Monitoring/IR Cameras/Borescopes)
- RF Tracking Systems
- AV Systems
- Parking Garage

Inventory

- OMB M-24-04 Requires Details:
  - Asset Identification- All devices and systems that meet the provided definition of covered IoT assets.
  - Asset Description- Including make, model and any relevant configurations. Assets should have a unique identifier, (serial or asset tag)
  - Asset Categorization- Function, Location, Type of system
  - Owner/Point of Contact- Person responsible for asset's management, administration, maintenance and security
  - Vendor/Manufacture Information- Contact information, support, contracts
  - Software and Firmware Versions- including patch management
  - Network Connectivity, Integration and API Information: IP Address, ACL/Firewall Rules,
  - Security Controls- ATO's, Standards, Protocols

Inventory

- Status of this inventory effort?
  - Automated sensor tools are being utilized to create a dynamic asset inventory of network connected assets. Today, VA also leverages manual inventory methods during the transition to automated tools. VA tracks approximately 139K medical assets via manual inventory methods. VA tracks approximately 55K SPS assets via manual inventory methods
  - VA is looking to expand the automated sensor tools to networks separated from the enterprise network to assist with the asset inventory.
  - Challenge-Inventory is constantly shifting and keeping the inventory up to date is critical.

Security Controls-Software & ATO

- Enhancement to the OT/IoT Enclave
  - Onboard All Systems- Software and Equipment
    - Utilize OIT-Technical Reference Model (TRM)
    - Utilize OIT-Enterprise Risk Analysis (ERA)
    - Cloud Based- FedRAM Approval Process
      - Very Challenging, Time Consuming and many smaller companies are challenged.
  - FISMA Compliance & Authority to Operate (ATO)- VA's Governance, Risk and Compliance (GRC) Tool- eMASS
    - Boundary's
      - Enterprise
      - Medical
      - OT Systems

Detection and Response

- Detection- Follows much of the standard plan for the enterprise network
  - Threat Detection
  - Anomaly Detection
  - Root Cause Analysis
- Response-Follows much of the standard plan for the enterprise network
  - Forensics Tools
  - Playbooks
- Understand OT networks are different than enterprise networks
  - Challenged for Updating (Test environments a limited)
  - Traffic is different
  - Tech Refresh rates are much longer and costly-Most are custom built systems
  - Built for the systems to talk and to last a long time-limited security

Where are we Going!

- Enhance the OT/IoT Enclave
- Enhance the FISMA Compliance & Authority to Operate (ATO)- VA's Governance, Risk and Compliance (GRC) Tool- eMASS
- Enhance Inventory Management of OT devices- Automate as much as we can
- Enhance Vulnerability and ways to patch OT system (Limit patching one-by-one)
- Enhance Standard Operating Procedures for like systems to streamline onboard at each facility
- Enhance standard management of air-gapped systems
- Explore Additional ways to manage vulnerabilities when patches are not practical or avaliable