Health Industry Cyber Security Practices:
Managing Threats and Protecting Patients (HICP)

Attacks on Network Connected Medical Devices

What is a Network Connected Medical Device?

The Food and Drug Administration (FDA) defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them; intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease." If compromised, connected devices such as Magnetic Resonance Imaging (MRI), Positron Emission Tomography (PET) scans, vital sign monitors, etc. can be an attack vector or source of a venerability to your network as well as directly alter the readings, or operations, of the devices themselves.

Real-World Scenario:

A threat actor gains access to a healthcare provider's computer network through an email phishing attack. The actor proceeds to take command of a file server to which a heart monitor is attached. While scanning the network for devices, the threat actor takes control (e.g., power off, continuously reboot) of all heart monitors in the Intensive Care Unit (ICU), putting multiple patients at risk.

Impact

As you see in this scenario, medical technology is vital for managing the health of our patients, and their operations at clinical grade performance is critical.

How Can HICP Help?

The publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector. The material on this flyer is a section of the publication that examines cybersecurity threats and vulnerabilities that affect the healthcare industry.

Staying Resilient to Network Connected Medical Devices

Know your organization's protocols in case of a potential shutdown or attack against medical devices. Help patients and staff by understanding the processes and procedures which can help mitigate the impacts. That means asking:

- Who is responsible for working with manufacturers to confirm security settings and software updates are maintained properly on each device?
- What additional security controls and monitors be put in place to protect each device?
- How will our staff and patients be notified if medical devices are compromised?
- What is our plan if medical devices are compromised and how will patients notify us if they suspect a compromise?

When To Ask About Network Connected Medical Device Attacks

Knowledge of your organization's protocols for potential attacks on medical devices shouldbe shared during new hire orientation, security training or both. Clinicians should understand the risks that cybersecurity threats of medical devices pose to patient safety and the specific controls in place to reduce those risks.Each organization should have IT security professionals to help answer any questions on the policy and governance associated with medical devices. If your organization does not, ask your supervisor for information and/or resources allowing you to learn more about the threat. Vendors or manufacturers of medical devices may need to be engaged to understand vulnerabilities, risks, and appropriate protection and response measures.

How Can You Mitigate Network Connected Medical Device Attacks?

Each individual threat discussed in the HICP publication provides threat specific mitigation practices. The table below lists the medical device attack mitigations along with a quick reference key to help locate further information in the HICP documents. The mitigation practices are covered in greater detail in the technical volumes included in the publication: Technical Volume 1 for Small Organizations and Volume 2 for medium and large organizations.

Network Connected Medical Device Attack Mitigation Practices to Consider
Establish and maintain communication with medical device manufacturer's product security teams **(9.L.A)**
Patch devices after patches have been validated, distributed by the medical device manufacturer, and properly tested **(7.S.A, 9.M.B)**
Assess current security controls on networked medical devices **(9.M.B, 9.M.E, 9.S.A)**
Assess inventory traits such as IT components that may include the Media Access Control (MAC) address, Internet Protocol (IP) address, network segments, operating systems, applications, and other elements relevant to managing information security risks **(9.M.D)**
Implement pre-procurement security requirements for vendors **(9.L.B)**
Engage information security as a stakeholder in clinical procurements **(9.L.B)**
Use a template for contract language with medical device manufacturers and others **(9.L.B)**
Implement access controls for clinical and vendor support staff, including remote access, monitoring of vendor access, multi-factor authentication (MFA), and minimum necessary or least privilege **(9.M.C)**
Implement security operations practices for devices, including hardening, patching, monitoring, and threat detection capabilities **(9.L.B)**
Develop and implement network security applications and practices for device networks **(6.S.A, 9.M.E)**

Key: 1-10 = Cybersecurity Practice | S = Small (Tech Vol 1) | M = Medium (Tech Vol 2) | L = Large (Tech Vol 2) | A-Z= Respective Sub-Practice

Example: "1.S.B Education": "1" refers to the cybersecurity Practice "Email Protection System" | "S" refers to Small size organization | "B" refers to the sub practice for small size organization within the Email Protection System – Cybersecurity Practice, which in this case is "Education"

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication at hhs.405d.gov or email us at CISA405d@hhs.gov. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram!