Transcript: Attacks Against Networks Connected Medical Devices

HHS 405(d)
Aligning Health Care Industry Security Approaches

Imagine this: A physician's office is experiencing disruptions in their equipment and is unable to provide care to its patients that rely on equipment to give timely and accurate information. Cyber-attackers have gained access to the office's network and scanned for connected devices that can put a patient's safety at risk.

Due to the attack, patient safety has been compromised at the office. The physician and their security contact have made the hard decision to refer patients to other offices and taken steps to move critical patients to another facility until the breach has been contained and the facility is deemed safe.

Attacks against network connected medical devices is a growing threat for practices and facilities of all sizes. This threat can start from access gained by an attacker from a simple social engineering attack.

This threat causes short-term and long-term issues for the practice or facility. Doctors unable to provide treatment because of malfunctioning equipment could lead to complications during surgery or other patients not receiving the attention that they need.

The practice may also suffer financial and reputational loss as a result of an attack against their medical devices connected to the network. If patients feel that their safety is at risk due to an unprotected facility, the practice could lose patients to other facilities or gain a bad reputation as a unsafe care facility.

So, how can you get ahead of these attacks and secure your 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 impact.

Ask:

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 need to be put in place to protect each device?

What is our staff's plan if network connected medical devices are compromised and how will patients notify us if they suspect a compromise?

You can:

Establish and maintain communication with medical device manufacturer's product security teams.

Assess current security controls on network connected medical devices.

Engage information security as a stakeholder in clinical procurements.

The best way to prevent attacks against network connected medical devices is to maintain consistent communication with your organization's IT or cybersecurity professionals and implement up-to-date cybersecurity policies.

The Department of Health and Human Services, or HHS for short, and the public-private partnership known as 405(d) are committed to aligning health industry cybersecurity approaches by creating, managing, and leading all industry-led processes to develop consensus-based, industry tested guidelines, practices, and methodologies to strengthen the health sector's cybersecurity posture against cyber threats.

Loss or left of equipment or data is one of the five threats identified in the HHS 405(d) publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), which

aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector.

Each individual threat discussed in the HICP publication provides threat specific mitigation practices, such as those provided earlier.

Additionally, the HHS 405(d) Program has more resources like other publications, awareness products, and outreach-focused social media platforms and events to keep your organization cyber safe, which keeps your patients safe.

No matter what role you serve in your organization, the 405(d) website at 405d. hhs.gov has resources to help you protect your organization and its patients from cyber threats.

As healthcare industry professionals, the best way for us to stay vigilant is for everyone, including you, to play a part and remember that Cyber Safety is Patient Safety.

Produced by the U.S. Department of Health and Human Services at Taxpayer expense.