How to Protect Against Threats to Interconnected Medical Devices

Interconnected medical devices, or the Internet of Medical Things (IoMT), are revolutionizing healthcare by improving patient monitoring, diagnosis, and treatment. But this digital integration also introduces significant cybersecurity risks. With over seven million IoMT devices anticipated by 2026, the attack surface is only expanding. While wearable heart monitors, smart inhalers, and connected imaging devices undoubtedly enhance patient care, insufficient security measures make them prime targets for malicious threat actors.

Common Attributes of Interconnected Medical Devices

Outdated Software and Firmware

Many IoMT devices run older, unsupported operating systems, making them prime targets for exploitation.

Lack of Encryption

Insufficient encryption can make data transmission between devices and servers susceptible to interception.

Unpatched Vulnerabilities and Exposures

Critical components like nurse call systems and infusion pumps often harbor unpatched vulnerabilities.

Multiple Attack Vectors

The interconnected nature of IoMT devices means that a breach in one device can potentially give attackers access to the broader network.

Insufficient Security Protocols

Many IoMT devices weren't designed with robust security in mind, leaving them exposed to various threats.

Consequences of Attacks on Interconnected Medical Devices

Disruptions to Patient Care

Attacks can lead to inoperable medical devices, delaying diagnoses and treatments, and potentially increasing patient mortality rates.

Financial Losses

Costs associated with cyberattacks include ransom payments, legal fees, system recovery, and loss of business.

Data Breaches and Privacy Violations

Exposure of sensitive patient data can result in legal consequences and loss of patient trust.

Operational Downtime

Healthcare services can be severely disrupted, leading to postponed appointments, services, and prescriptions.

Regulatory Penalties

Non-compliance with cybersecurity regulations can result in significant fines and penalties.

Why You Might Be Vulnerable to Threats Against Interconnected Medical Devices

High Interconnectivity
Extensive use of interconnected devices increases the attack surface.

Outdated Technologies
Many devices operate on outdated or unsupported software.

Resource Constraints
Limited budgets and staff for cybersecurity measures.

Lack of Awareness
Insufficient security awareness training regarding cybersecurity risks.

Complex IT Environments
Larger hospitals have complex networks that can be difficult to secure.

Insufficient Patch Management
Delays in applying security patches to devices.

Solutions to Better Fight Threats to Interconnected Medical Devices

- ☐ **Monitor and Manage Vulnerabilities**
  Implement continuous threat exposure management tools like breach and attack simulation (BAS) and vulnerability scanners.
- ☐ **Encrypt Data**
  Ensure all data transmitted between devices and servers is encrypted.
- ☐ **Patch and Update Software Regularly**
  Keep all devices updated with the latest security patches.
- ☐ **Adopt Managed Endpoint Detection and Response (EDR)**
  Utilize a managed EDR solution to monitor, detect, and respond to threats in real time.
- ☐ **Introduce Security Awareness Training (SAT)**
  Regularly train your healthcare staff on cybersecurity best practices and security awareness.
- ☐ **Create an Incident Response Plan**
  Develop a comprehensive plan to quickly address and mitigate cyberattacks.
- ☐ **Perform Regular Audits**
  Conduct security audits and penetration testing to identify and address your vulnerabilities.
- ☐ **Segment Networks**
  Separate IoMT devices from other critical network components to limit the spread of attacks.

The interconnectivity of medical devices brings both tremendous benefits and significant cybersecurity risks. By understanding common threats and their potential consequences, as well as implementing comprehensive security strategies, you can better protect your digital infrastructure and, ultimately, your patients' well-being.

Want to go deeper into threats against interconnected medical devices?

Check out our blog for more insights and strategies.

HUNTRESS