Cybersecurity for Medical Devices

What is Medical Device Cybersecurity?

Cybersecurity for medical devices is vital for protecting both the data and lives of patients as well as protecting medical institutions from ransomware attacks. With the evolution of medical devices and their connectivity, cyberthreats have continued to evolve in tandem creating new risks.

Why Is Cybersecurity for Medical Devices So Important?

The risks in medical device cybersecurity are multifaceted, emphasising the need for up-to-date certifications and standards as well as undergoing cybersecurity evaluations. Effective risk management involves **enhancing life cycle processes** and conducting **rigorous penetration testing** to identify vulnerabilities and strengthen security.

Cybersecurity Risks and Requirements for Medical Devices

The cybersecurity risks for medical devices are:

- **Regulatory requirements:**
  Medical devices are subject to **stringent regulations** by bodies such as the **FDA** in the United States, the **EMA** in Europe, **NAPA** in China, and other regional regulatory agencies. These regulations require adherence to specific cybersecurity standards and guidelines to ensure devices are safe from hacking and other cyber threats. Non-compliance can result in **severe penalties, recalls, or bans.**

- **Patient safety:**
  Cybersecurity flaws in medical devices can directly **jeopardise patient safety.** If a device such as a pacemaker or insulin pump is breached, it could malfunction, delivering incorrect treatment doses or failing at critical moments.

- **Privacy and Disruptions:**
  Since medical devices often store and transmit sensitive health information, a security breach can **expose personal health records**, leading to identity theft and **loss of patient confidentiality.** This is a typical risk in ransomware attacks, where **malicious actors encrypt critical data** and demand a ransom to unlock it. Such attacks not only compromise patient privacy but also **disrupt the essential operations of healthcare systems**, underscoring the critical need for robust cybersecurity measures.

Cybersecurity Medical Devices Standards and Guidelines

Given the risks involved, medical device cybersecurity is tested against **stringent international and national standards.** Regulatory bodies around the world have published guidelines concerning the regulation of medical device cybersecurity and outline the tests that they need to undergo to reach markets. At Applus+ Laboratories, we can support you with the following standards:

- **MDCG 2019-16 EU Guidance on Medical Device Cybersecurity:**
  Ensuring the integrity and confidentiality of medical device data across the European market.

- **USA / FDA Guidance on Cybersecurity in Medical Devices - Quality System Considerations and Content of Premarket Submissions:**
  Guidelines for incorporating cybersecurity measures from design to deployment within the U.S. regulatory framework.

- **IEC TR 60601-4-5 Standard for Medical Device Cybersecurity:**
  A technical roadmap for implementing global cybersecurity standards in medical devices.

- **IEC 81001-5-1 Standard for Health Software and Heath IT Systems Security Activities in the Product Life Cycle:**
  Strategies for maintaining cybersecurity throughout the device's operational life, applicable worldwide.

Why choose Applus+ Laboratories for Cybersecurity for Medical Devices?

Applus+ Laboratories offers **comprehensive cybersecurity testing services** for evaluating medical devices and we have many years of experience doing **cybersecurity evaluations** and carrying out **penetration tests** on all kinds of Targets of Evaluation (TOEs).

Security Testing

Applus+ Laboratories offers extensive penetration testing services to assess the resilience of systems against attacks and unauthorised access. By performing cyberattack simulations, we evaluate vulnerabilities in medical devices across various components:

On Hardware

State-of-the-art attacks and ad-hoc tools made by lab experts:

- Fault Injection
- Side Channel
- Reverse Engineering
- Design Review
- Logical Attacks
- IC/SoC Attacks
- PCB HW Hacking
- Biometrics Attacks

On Software and Firmware

Strong background in embedded systems, secure boot, TEE and white box crypto:

- Binary Reverse Engineering

- Static Attacks
- Source Code Audits
- Debugging
- Fuzzing
- Dynamic Tamper / Hooking
- SW Timing Analysis and CCA
- Symbolic Execution

On Communication Protocols

For IP stack protocols, industrial systems and proprietary protocols:

- All layer attack (OSI Model) including customised HW to stimulate at lower layers (wired and wireless protocols)
- Fuzzing
- Dynamic Tamper / Hooking

Our expertise in cybersecurity further enhances the security measures we recommend. Penetration testing activities conducted in our expert lab not only help to strengthen product cyber resilience. The report generated by Applus+ Laboratories experts can be used as a **proof of compliance** with cybersecurity requirements mandated by regulatory bodies worldwide such as FDA in the USA.

Compliance Verification

Our teams can also support manufacturers worldwide verifying if their product **complies with specific standards or guidelines** requested by regulatory bodies. Our certificate of compliance facilitates product readiness for the approval process on various markets.

Contact Applus+ Laboratories to test and **certify the cybersecurity of your medical devices** to get your product to market as quickly as possible.