BioSpectrum the business of Bio & Health Sciences

How MedTech industry can benefit from adage of ‘Prevention Is Better Than Cure’

20 September 2021 | Views

Understanding the need for proactive cyber risk assessment and security posture to combat cyber attacks

The phrase *'prevention is better than cure'*, often attributed to the Dutch Northern Renaissance philosopher Desiderius Erasmus forms the fundamental principles of our approach to modern healthcare and maintaining a healthy lifestyle. Technology has today made deep inroads into the healthcare sector transforming the practice of modern medicine. Health care systems are now leveraging the potential of the Internet of Medical Things (IoMT) and Internet-connected devices are being designed to enhance efficiencies, diminish costs, and drive better results.

The Medtech industry has been one of the key contributors to the healthcare ecosystem playing a strategic role in fostering the change of health care delivery towards better health outcomes. With India being ranked among the top 20 markets for medical devices worldwide, according to IBEF, the current market size of the medical devices industry in India is estimated to be nearly $10 billion and poised for significant growth in the next five years, it is expected to reach $50 billion by 2025.

That said, the proliferation of connected smart medical equipment devices such as pacemakers, insulin pumps, drug infusion pumps, cardiac implants, or other vital monitoring systems, are also making healthcare more prone to cyberattacks and data breaches that directly endanger the patients’ privacy and safety. As per McAfee’s Cloud Adoption and Risk Report – Work From Home Edition released in May last year, healthcare is the second most target industry followed by manufacturing when it comes to external cloud threats.

Vital yet vulnerable

McAfee's Enterprise ATR team recently partnered with Culinda and identified a set of vulnerabilities that could be used by a malicious actor to modify a pump's configuration while the pump is in standby mode in the B Braun Infusomat Space Large Volume Pump and the B Braun SpaceStation. These vulnerabilities could permit the hacker to conduct remote network attacks which resulted in a modified and unexpected amount of dose being given to a patient.

What makes the security of these devices a pressing issue is the network effects associated with connected platforms without proper cybersecurity controls. This can lead to catastrophic security breaches, as the majority of them use multiparty code including open source without actually analysing them for vulnerabilities. Denial of service attacks, theft of the patient's data, lateral access to other parts of the organisation's network, and device malfunction leading to patient death in some cases are some of the most common types of cyber-attacks that stem from device vulnerabilities. Further, the medical devices that are currently used by healthcare organisations were potentially designed, way before the MedTech industry critically started looking at it from a cybersecurity standpoint. As a result, hospitals today, are using older devices with outdated software, hardware, and protocols, unprotected from vulnerabilities yet holding sensitive, personal, and life-sustaining information.

The complexity and size of hospital operations, coupled with the existence of outdated systems, further hinder the employment of effective cybersecurity strategies. The obvious question, therefore, is how to change the landscape of cyber threats in MedTech and combat attacks as there is more at stake than the privacy of data? The answer lies in ensuring security at every level, making it a significant and critical component of the entire infrastructure.

Building cyber resilience

With the advent of technology, it has become convenient to identify medical devices, understand their vulnerabilities, and provide non-intrusive security on the network. Some key methods that can be followed are:

- **Security is key** - Security must now be baked into the entire process of manufacturing a medical device, and to be effective, security protocols need to be adhered to by all the businesses that will use the solution across the entire lifecycle of a device
- **Assess and address device vulnerabilities-** Access to home peripherals, including home IoT devices, should be scrutinised closely. The objective is to lessen the threat profile for VPN-connected devices to maximise user security while also minimising user disruption and ensuring a smooth user experience
- **Controlled access to valuable data -** It is essential to know who's been granted access to sensitive data. Monitor and audit actions of privileged users closely
- **Provide breach training –** Every employee must be trained on handling security breaches and the accurate ways to report them, as well-timed action by an informed employee can help thwart data from being compromised further
- **Invest in cybersecurity -** Upgrading systems and processes is the need of the hour as most of the cybersecurity systems utilised by healthcare organisations are outdated and incapable to fend off cyberattacks

Marching ahead to secure the future

Just how healthcare's goal is prevention and wellness, cybersecurity's is avoidance and resilience. Information sharing in a hyper-connected world is a new reality, thus making data security critical for device manufacturers, care providers, and health consumers. Like the adage 'prevention is better than cure', they too will have a crucial task of upping their security measures before their patient's data or trust is compromised.

Venkat Krishnapur, VP of Engineering and Managing Director, McAfee Enterprise India, Bengaluru