HealthManagement
Promoting Management and Leadership

Cybersecurity Risks of Implantable Medical Devices

As the healthcare industry embraces digitalisation, it reaps numerous benefits, from enhanced patient care to streamlined operations. However, this shift has also exposed the sector to significant cybersecurity risks. One of the most alarming trends is hackers' targeting of implantable medical devices. These devices, which are designed to save lives, can also be manipulated to cause harm if their vulnerabilities are exploited. This article explores why hackers target these devices, which implants are most at risk, their common vulnerabilities, and what healthcare providers can do to secure them.

Why are Hackers Targeting Implantable Medical Devices?

The healthcare sector has become a lucrative target for cybercriminals due to the high value of the data it holds. Medical records can sell for up to $250 each on the dark web, making them far more valuable than payment card information. This financial incentive drives hackers to continually attack healthcare systems. According to reports from the U.S. Health Sector Cybersecurity Coordination Center and the Office of Information Security, healthcare data breaches have been on the rise since 2012, with a significant increase from 2018 to 2021. Despite stringent privacy and security regulations, these breaches exposed 385 million patient records from 2010 to 2022.

Hackers are now exploiting a new angle: implantable medical devices. These devices, such as pacemakers and insulin pumps, are connected to networks, making them vulnerable to attacks. By compromising these devices, hackers can threaten patients' lives, creating a powerful incentive for hospitals to pay ransoms. The ability to directly impact patient health makes these attacks particularly dangerous and effective.

Which Medical Device Implants Are Vulnerable to Attacks?

Several types of implantable medical devices have demonstrated vulnerabilities to cyberattacks. Pacemakers were among the first to receive a cybersecurity-related recall from the U.S. Food and Drug Administration (FDA). In 2017, the FDA warned that pacemakers manufactured by St. Jude Medical had a critical flaw that could allow attackers to drain their batteries, alter heartbeats, or administer inappropriate electric shocks.

Other intracardiac devices have also been found to have severe vulnerabilities. In 2023, the Cybersecurity and Infrastructure Security Agency highlighted a critical flaw in a Medtronic device, rated 9.8 out of 10 in severity by the Common Vulnerability Scoring System. Attackers could exploit this flaw to steal, delete, or modify device data and, more alarmingly, to tamper with or shut down the device remotely.

Neural implants are another category at risk. Though real-world attacks on these devices are rare, the possibility exists. Hackers could theoretically exploit vulnerabilities in their wireless communication protocols to induce pain, modify behaviour, or cause psychological distress. While the known attacks have primarily targeted insulin pumps, cardiac defibrillators, and pacemakers, the range of potential targets could expand if attackers find these devices profitable or easy to compromise.

Common Vulnerabilities in Medical Device Implants

Implantable medical devices often share similar vulnerabilities, despite the FDA's 2023 mandate for stricter security guidelines. The U.S. Government Accountability Office reports that each medical device has an average of 6.2 vulnerabilities. Some of the most common issues include:

- Insecure Default Configurations: Manufacturers often publish administrative passwords and hardware details to help providers and patients. If these default settings are not changed, attackers can easily access the devices.

- Unsecured Communications: Many implantable devices use unsecured communication protocols to transmit data. These protocols can be intercepted, providing a gateway for attackers into hospital networks.
- Unpatched Software Vulnerabilities: Software in medical devices often contains bugs that go unnoticed. Even when detected, these vulnerabilities can pose risks if not promptly patched.
- Manual Radio Interference: Attackers can use publicly available information on radio frequencies to intercept and manipulate data being transmitted by medical devices.

What Can Healthcare Providers Do to Secure Implants?

To mitigate these risks, healthcare providers need to implement robust cybersecurity measures. Here are some essential steps:

- Multi-Factor Authentication (MFA): Requiring MFA can significantly limit attackers' ability to access device data or alter settings, even if they obtain passwords.
- Password Updates: Regularly updating passwords and changing default credentials can protect devices from brute-force attacks and data breaches.
- Penetration Testing: Simulating cyberattacks through penetration testing can help identify and address security gaps in a controlled environment.
- Data Encryption in Transit: Encrypting all data in transit prevents attackers from intercepting and manipulating it.
- Automatic Updates: Ensuring that devices automatically receive software patches can drastically reduce the number of exploitable vulnerabilities.

The healthcare industry must prioritise cybersecurity to protect its patients. Implantable medical devices, while life-saving, present new vulnerabilities that hackers are eager to exploit. By adopting stringent security measures, healthcare providers can safeguard these devices against cyberattacks, ensuring they remain tools for healing rather than instruments of harm. Working together, providers, patients, and manufacturers can create a secure environment where the benefits of digitalisation do not come at the cost of patient safety.

Source: HITConsultant

Image Credit: iStock

Published on : Thu, 18 Jul 2024