Today, almost all sectors are dependent on technology. While technology expands the functionality of individual items, it can also introduce novel threats. These include security breaches, data leaks, partial/total failures, etc.

During the past few years, the medical sector has seen an increase in interconnected medical devices. Even though devices are built medically sophisticated, they are not equipped with anti-cyber attack tools (Glisson, et al. 2015). A combination of inadequate training and lack of anti-cyber-attack tools has left a vast number of medical devices vulnerable to cyber attacks.

Glisson, et al assembled a team of young undergraduate students in order to investigate the viability of compromising a mannequin training system focusing on the communication between the medical mannequin and the software (Muse) controlling it. Even though this team did not have any prior training in penetration testing tools, they still managed to disrupt the mannequin's function using BackTrack 5 software only.

Initially, by using a BackTrack 5 r3 live CD, the students performed a brute force attack against the mannequin's WPS PIN numbers.
WIFI Protected Setup (WPS) is a function almost all modern wireless devices are equipped with. It only works if the network is protected using WPA Personal or WPA2 security protocols. Essentially, if activated on one device, a second device can search for all available WPS setups around and connect to the first device without the need of entering a password (Techinpages, 2019).

Additionally, students using the BackTrack 5 r3 live CD searched for all nearby access points and performed a Denial of Service (Dos) attack against the mannequin's and Muse connection.

In both attacks students managed penetrate the device; they cracked the WPS PIN within a little more than 2 hours and successfully disrupted the connection between the mannequin and its software.

Threats and Vulnerabilities Mitigation

- WPS normally works in two ways:
    1. By transmitting a simple PIN number.
    2. By transmitting the same complex passphrase in WPA/WPA2 security protocol.

  By disabling the PIN option, it would take years for the BackTrack software to crack the WPA password as it consists of multiple characters (lower/upper keys, symbols and numbers). Otherwise, for additional security, WPS should be disabled altogether.

- A firewall should be installed in order to block recognised DoS attacks (Norton, 2020). If a device runs a ROM memory, a front-end hardware device could be installed. This device could be integrated into the network and operate as a proxy. All packages would go through this device first and if "cleared", the proxy would forward the package to the components of the network (Norton, 2020).

- Cyber security awareness trainings should be provided to all personnel operating IT and network connected IT devices, in order to identify any abnormal or malicious behaviour and mitigate further harm.

References:

Glisson, W.B., Andel, T., McDonald, T., Jacobs, M., Campbell, M. and Mayr, J., 2015. Compromising a medical mannequin. arXiv preprint arXiv:1509.00065.

Norton (2020) What are Denial of Service (DoS) attacks? DoS attacks explained Available from: https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html [Accessed 18 May 2021].

Techinpages (2019) What is WPS Available from: https://www.technipages.com/what-is-wps [Accessed 18 May 2021].