Student: Edward

In the journal “Compromising a Medial Mannequin” the consensus is that the medical field needs a major overhaul with regards to security, this includes application security but also physical security which can be access to sensitive equipment used by medical staff and patients and equipment like routers, switches, and computers.

It was mentioned by the FBI “the health care industry is not technically prepared to combat against cyber criminals’ basic cyber intrusion tactics” (Federal Bureau of Investigation 2014)”.

With little or no systems in place to ensure failed login attempts are captured or alterations to equipment are captured by means of alerts, medical facilities are operating blind and are unaware of attacks that are happening or can happen. Equipment used by patients such as pace-makers or insulin pumps that have rely on WIFI communication using weak protocols can have detrimental effects on patients if for example, an insulin pump is adjusted to input less or more insulin into a patient, or a pacemaker is adjusted that can cause the heart to beat abnormally and could result in a heart attack.

Vendors that create software for the medical equipment should look at using stronger protocols in WIFI and need to invest in testing the applications before rolling it out. Protocols such as Wired Equivalent Privacy (WEP) was introduced to prevent Man-in-the-Middle-attacks but was with age, computers have become more powerful and this protocol has become insecure and should no longer be used (Gregory Manley, 2020). WI-FI Protected Access 2 (WPA2) that uses the protocol Advanced Encryption Standard (AES) or WPA3 protocols should be looked at to improve security on these devices to ensure that they are protected (Eric Geier, 2018).

To assist with Denial-of-Service Attacks (DOS) (Paloalto networks, 2021), systems such as intrusion detection system (IDS) and intrusion prevention system (IPS) can be implemented to monitor traffic on the network and raise alerts on anything detected (Anon, 2021)

Cyber Training is vitality important for medical staff as they can alert of anything strange happening and potentially stop an attack before it is too late. There are many campaigns available to teach staff on cyber threats. According to Gartner (2021), “85% of data breaches involve a human element”.

One other way to mitigate risk is by principle of least privilege (CyberArk, 2021) This means only granting access to staff based on what they need to perform their jobs.

Thank you, Edward, for an insightful post. I agree with your points that vendors need more robust WIFI protocols and invest in testing applications of medical devices. Ultimately securing medical devices protect human life, health and wellbeing (Sametinger et al., 2015). Therefore, software vendors have a vast responsibility to ensure the privacy of sensitive health information and maintain the CIA triad (Troncoso, 2019). This is further supported that particularly in the case of software issues; the FDA saw many recalls of devices (Kramer et al., 2012). It was not uncommon to see this whereby vendors needed to update or improve the applications. Examples can be taken from companies such as the Mayo Clinic who introduced contract language with vendors (Loughlin, 2016). Whilst this initially saw a hostile reaction from vendors, Mayo Clinic felt it was necessary. The language used would gain affirmation from vendors that they had developed and maintained a comprehensive security program. This would create a policy that would align with industry standards and include identifying and assessing external risks to medical devices and setting limits on the amount of data that can be stored. Whilst this was a challenge for both parties, it meant that vendors began to send devices for testing before purchasing and would make changes later to improve the security. This would allow a better product to be made, be more cost-effective for the company purchasing, and healthcare provisions would be enhanced.

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K. & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLoS ONE,* 7, (7): e40200.

Loughlin, S. (2016). In Contracts with Device Vendors, Mayo Clinic Emphasizes Security. *Biomedical Instrumentation & Technology,* 50, (1): 53-55.

Sametinger, J., Rozenblit, J., Lysecky, R. & Ott, P. (2015). Security challenges for medical devices. *Communications of the ACM,* 58, (4): 74–82.

Troncoso, C. (2019). Privacy & Online Rights Knowledge Area Issue 1. Available: https://www.cybok.org/media/downloads/Privacy__Online_Rights_issue_1.0_FNULPeI.pdf [Accessed 13 November 2021].