Security Breaches and Issues

The major threat and vulnerabilities discussed in the paper are security threats and issues of medical devices that involve identification, monitoring, and control. The vulnerabilities include network and operating system vulnerabilities. From the reading, the health care industry is not technically prepared to fight against cyber criminals’ intrusion tactics due to insufficient funds. Shabani and Munir (2020), in their research, found that security threats and vulnerabilities in hospital increases because most of the technique used to prevent attack are outdated and rudimentary. There has been an increased number of exploitable vulnerabilities and failures of medical devices in the last five years. The mannequins used in the medical hospital are at risk of cyber-attack. The mannequins which are likely to be attacked include the network security and protocol (Andel et al., 2015). In this case, the security was breached using an open brute force attack against the router Personal Identification Number (PIN) while the network protocol was attacked through a denial of services attack. Another mannequin attack involved training facility information. This shows that the medical training is breached, which affects the long-term ripple on the medical profession, which can adversely impact thousands of lives due to incorrect analysis of life-threatening data by medical personnel.

Security threats and issues from the reading can be mitigated by implementing encryption to impact the longevity and performance of medical devices enhance wireless communication that potentially increases the exposure to attack. Encryption mitigation will involve analyzing medical devices by encrypted traffic in the network that identifies the attack and evaluates mitigation techniques such as obfuscation (Baldini et al., 2020). Also, health care addressing the issue of security will involve the collaboration between security and medical communities and industries in terms of devices and policies to put in place. Hospitals should secure implantable medical devices protected by jamming the incoming and outgoing signals. It will involve achieving the analytical solution of jamming to allow security accountability to multiple separate devices that act as the entry to the authorized devices (Adem, Hamdaoui, and Yavuz, 2016). The medical hospital should use a combination of modeling techniques with wireless body area networks to provide storage and process time (Andel et al., 2015). In this case, the data collected for devices to measure like body temperature or heartbeat should be transmitted to the mobile devices to establish security to the storage area and the transfer of data.

Reference list

Adem, N., Hamdaoui, B. and Yavuz, A., 2016. Mitigating jamming attacks in mobile cognitive networks through time hopping. *Wireless Communications and Mobile Computing*, *16*(17), pp.3004-3014.

Andel, T., Campbell, M., Glisson, W., Jacobs, M., Mayr, J. and McDonald, J., 2015. Compromising a Medical Mannequin.

Baldini, G., Hernandez-Ramos, J.L., Nowak, S., Neisse, R. and Nowak, M., 2020. Mitigation of privacy threats due to encrypted traffic analysis through a policy-based framework and MUD profiles. *Symmetry*, *12*(9), p.1576.

Shabani, N. and Munir, A., 2020, July. A review of cyber security issues in hospitality industry. In *Science and Information Conference* (pp. 482-493). Springer, Cham.