Responses to my initial post

1.

Post by **Beran Necat**

Re: Initial Post

Hi Jonathan,

Good use of references, well researched, and good use of alternative viewpoints - as you say technology is not always the first or only answer. Well-trained staff and strong processes can also help - maybe training is needed for patients too in some instances?

Regards, Beran

Reply

2.

Post by **Muhammad Qasim**

Peer Response

Thank you for the great discussion. The post has reviewed the article “Compromising a medical mannequin” well highlighting how severe the effects of cyber attacks threats are to practitioners and patients. Medical devices depend on software for patient care ranging from radiation therapy planning to pharmaceutical compounding to the automated diagnosis of disease with mobile medical apps. Meanwhile, the medical community has observed an uptick in reported security vulnerabilities in medical device software raising doubts of cybersecurity preparedness. The discussion has also talked about how the FDA MAUDE does not capture adverse events such as lack of or impaired availability of function when malware infects a medical device's operating system. The FDA's own disclaimer explains that the MAUDE database is qualitative rather than quantitative. MAUDE is incomplete with underreporting and reporting bias (Andel et al., 2015). A medical device infected with malware can stray from its expected behavior. For instance, malware can cause a device to slow down and miss critical interrupts. When this happens on a high-risk pregnancy monitor, healthcare professionals could no longer trust the integrity of the sensor readings and depend on backup methods Vividly discuss the vulnerabilities and the possible prevention methods in detail.

References

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

Reply

3.

Post by **Haseeb Abdulhak**

Peer Response

Thank you, Jonathan, for your informative post, you provide an excellent point about education and training how they are an important factor for countermeasure the threats in the cyber security age. Having a good and comprehensive IT security policy is a good thing, however, this is not enough if the people lack cyber security awareness and know what the risks and consequences are, therefore, without educating your employee about such as malware and their capabilities to harm the system, preventing them to be spread on the network will be a challenge (Sungard Availability Services, 2021).

It is needed to change all device's default usernames and passwords. The mirai botnet attack which is a DDoS attack in October 2016 in a simple way was able to gain access to many of CCTVs, Cameras, and routers that were connected to the Internet by trying login with default user and password, which are equipped with devices as default (Fruhlinger, 2018).

References

Fruhlinger, J. (2018) The Mirai botnet explained: How IoT devices almost brought down the internet. Available from: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html [Accessed 20 November 2021]

Sungard Availability Services. (2021) Educate employees to reduce cyber incidents. Available from: https://www.sungardas.com/en-us/blog/educating-employees-on-cyber-security [Accessed 21 November 2021]