PEER- RESPONSE

By (Student’s Name)

Course

Professor

University

City and State

Date

Peer - Response to an Article

Glisson et al., 2015 discuss the reliance on technology in medical training equipment and the cyber security risks and dangers resulting from this reliance. I agree with the authors that increased reliance on technology poses a significant risk to hospitals. Although incorporating technology into the health industry results in improved precision in healthcare, it is also susceptible to cyber security risks and perils. As such, breakthroughs in cybersecurity safeguards are still needed (Argaw et al2020, p.2). The article focuses on the viability of a production-deployed medical training mannequin. Thousands of people will be affected if a medical device is compromised since medical professionals will erroneously analyze life-threatening data. Notably, data breaches are not just a source of anxiety and difficulty for security professionals because they also affect the patients, stakeholders, organizations, and enterprises (She et al 2020, p.133).

The study also analyzes potential weaknesses for the medical mannequin arising from brute force assaults and Denial of Service (DoS). Although Denial of Services cannot be eradicated, they can be minimized using various methods including blocking approaches that mitigate DoS attacks by restricting the ports to which hostile hosts are connected or discarding malicious traffic (Imran et al 2020, p. 445). Additionally, the attacks can be mitigated by investing in reliable security mechanisms and investing in up-to-date antivirus software, which will facilitate the identification and prevention of any viruses and malware that might affect the network. Tan et al (2021, p. 5) proposes the installation of Grid-based honey as a security measure against brute force attacks. According to the authors, instead of denying access as a security defense system in mobile healthcare applications, the suggested Grid-based Honey Encryption generates an indistinguishable counterfeit patient's record that closely resembles the actual patients' records in light of each erroneous legitimate password speculation.

Reference List

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O’Leary, C., Eshaya-Chauvin, B. and Flahault, A., 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*(1), pp.1-10.

Imran, M., Durad, M.H., Khan, F.A. and Derhab, A., 2019. Toward an optimal solution against denial of service attacks in software defined networks. *Future Generation Computer Systems*, *92*, pp.444-453.

Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R. and Ahmad Khan, R., 2020, June. Healthcare data breaches: insights and implications. In *Healthcare* (Vol. 8, No. 2, p. 133). Multidisciplinary Digital Publishing Institute.

Tan, S.F., Lo, K.M.C., Leau, Y.B., Chung, G.C. and Ahmed, F., 2021, September. Securing mHealth Applications with Grid-Based Honey Encryption. In *2021 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)* (pp. 1-5). IEEE.