Collaborative Discussion 1 – Received Response – Austin Mundy

You brought up some great points within your post. Technologies in the world are evolving rapidly which opens them up to significant threats. An ENISA article reported that the healthcare industry was one of the five most target fields in 2020 (ENISA, 2020). The number of attacks will most likely continue to rise.

As for stopping brute force attacks, the ideas that you suggest are very effective. The general consensus for stopping brute force is complex passwords, two-factor authentications, and limited login attempts. Limiting login attempts can be problematic in medical environments, given that a critical device could be shut down at a critical moment (Sheridan, 2021). However, for medical training devices, such as a mannequin, that isn't a problem since there isn't a life-threatening threat. Another technique could be the implementation of packet inspection or IP filtering. Both of these techniques could be applied to both brute force attacks and Dos attacks. You bring up a good point about some solutions being very effective but economically not feasible. Healthcare systems are known to have some financial struggles. Otherwise, a more all in one device such as a next-generation firewall (NGFW), could be effective. It is an expensive device but contains several important devices such as IDS, IPS, and packet filtering all in one.

References:

ENISA. (2020) Main incidents in the EU and worldwide. Available from:

https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents [Accessed 20 November 2021].

Sheridan, E.(2021) Blocking Brute Force Attacks.Available from: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks# [Accessed 20 November 2021].