Collaborative Discussion 1 – Initial Post – Michael Geiger

The networking of end devices with networks and the Internet enable new and better possibilities, which can achieve great success, especially in the medical industry of implants. Along with the possibilities, there are also dangers associated with technical progress. Basu (2013) states that "Medical devices are becoming more networked every day, but the security requirements that should accompany any networking of a device are not keeping up."

The article “Compromising a Medical Mannequin” (Gilson, et al, 2015) deals with possible cyber threats and their technical aspects. Two threats could be identified in the project, brute force attacks and denial of service (DoS) attacks. While brute force attacks aim to obtain the access data by guessing the password and are based on the principle of try and error, DoS attacks aim to paralyze accessibility and communication through a flood of requests.

In the article, a successful brute force attack with the BackTrack5 program was achieved within a few hours. A DoS attack could also be carried out successfully in this way, which meant that no changes to the settings of the medical mannequin could be made during the attack.

There are a number of approaches to preventing brute force attacks, such as long and complex passwords, limited login attempts or the two-factor authentication. Deception-based security mechanisms is another approach. The aim here is to enable attackers to have comparably easy access to data in order to make them believe that they have achieved their goal, but only to provide fake data (Lijimol & Dileesh, 2020). This approach is based on the principle of the honeypot system (Wafi et al. 2017).

To prevent DoS attacks, the network can be expanded to process larger requests and data volumes. However, this approach encounters the problem that an infinitely large scaling is not possible and also does not make sense from an economic point of view. Another approach is the controller-agent model, which detects irregular and high inquiries from a source and prevents communication (Tupakula & Varadahajan, 2017).

References:

Basu, E. (2013) Hacking Insulin Pumps and Other Medical Devices from Black Hat. Forbes. Available from: https://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/?sh=b22535521f8e [Accessed: 09.11.2021]

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Sighealth. Available from: https://aisel.aisnet.org/amcis2015/HealthIS/GeneralPresentations/5/ [Accessed: 09.11.2021]

Lijimol, J. & Dileesh, E. (2020): Technique to Thwart Brute-Force Attack : A Survey. International Journal of Scientific Research in Science, Engineering and Technology. 7(1): 235-237. Available from: https://d1wqtxts1xzle7.cloudfront.net/65388723/6220-with-cover-page-v2.pdf?Expires=1636542213&Signature=gcfVJxBEQ~WBEWeW-8Tnw7nnZXrqi0LGxLEeP-LUUXV4rSWFsowZnQ0GoBytWIqVMQ1Ttxg4-jigsgBQjrgZuoJfmvmQnYFhPo21nPqT30Ylgw7jQ0P4uqqbAMD9Lm0S9GNQ2UvBeCKZcLKthBxtYnANdMayeokGPFalBAX-jSLVFzkDGM66hXhOIwlTZIp1xaK2X881trbjc6IZa7MvLVs2nAzNRLKQvBMgdlQ3POBK031jDfYa66iwBSV89fdupL8CRa9RdLwW3KGyx1CWNAJm6RYHgP8uAogLWq7uajneUKWNza8szXt4icB2fUpXvBIZSCh49JS5q7ZLMCFcBw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA [Accessed: 10.11.2021]

Wafi, H., Fiade, A., Hakiem, N., Bahaweres,R. (2017) Implementation of a modern security systems honeypot Honey Network on wireless networks. International Young Engineers Forum (YEF-ECE). Available from: https://ieeexplore.ieee.org/abstract/document/7935647 [Accessed: 10.11.2021]

Tupakula, U., Varadharajan, V. (2003) A Practical Method to Counteract Denial of Service Attacks. Available from: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.12.6606&rep=rep1&type=pdf [Accessed: 10.11.2021]