**Collaborative Discussion 1 – Summary Post – Michael Geiger**

The rapid technical development of medical devices must be viewed from two sides of the same coin. On the one hand, the technological achievements offer a multitude of possibilities in the medical monitoring and treatment of patients. On the other hand, cyber threats go hand in hand with the achievements and the technological embedding in medical devices, which have led to a massive increase in cyber attacks in the medical industry in recent years (ENISA, 2020).

All information technology systems, medical but especially due to their direct consequences for the affected patients, are subject to the mantra of the CIA, Confidentiality, Integrity and Availability, with the addition of Non-Repudiation. Since new developments often create unimagined possibilities, which can lead to new vulnerabilities and which are not recognized during development in the laboratory and testing in small research groups, these devices are often inadequately protected in terms of cyber security (Yaqoob et al., 2019). This makes such devices particularly susceptible to zero-day exploits. Retrofitting developed medical devices is often time-consuming and costly, especially since such devices can already be located in patients in the form of implants (Thomasian & Adashi, 2021).

However, there are already a large number of possible technologies for closing vulnerabilities in medical devices and preventing threats. This includes basic security aspects such as strong passwords, two-factor authentication and, depending on the use of the device, limited login attempts (Esheridan, 2021). Also the zero-trust architecture and the physical protection of the devices against malicious actions such as the removal of drives, USB and SSD ports can be viewed as a risk prevention, whereby the BIOS can be protected against manipulation by self-healing backups (Alexander, 2002).

Filters and firewalls such as packet filters, IP filters, proxy firewalls, intrusion detection systems (IDS) and intrusion prevention systems (IPS) represent further protective measures. Next generation firewalls offer many of these measures in one and, in combination with honeypots or deception-based security measures, can offer extensive protection (Zaki et al. 2021).

**References:**

Alexander, M. (2002) Mehtod and Computer for selfhealing BIOS initialization code. United States Patent. Available from: https://patentimages.storage.googleapis.com/3c/03/3f/9c965f81fc45b2/US6393559.pdf [Accessed: 26.11.2021]

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 26.11. 2021]

Esheridan (2021) Blocking Brute Force Attacks. Available from: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks# [Accessed 25.11. 2021].

Thomasian, N. & Adashi, E. (2021) Cybersecurity in the Internet of Medical Things. Health Policy an Technology, 10(3): 100549. Available from: https://www.sciencedirect.com/science/article/abs/pii/S2211883721000721 [Accessed: 25.11.2021]

Yaqoob, T., Abbas, H. & Atiquzzaman, M. (2019) Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices. IEEE Communications Surveys & Tutorials. 21(4): 3723-3768 Available from: https://ieeexplore.ieee.org/document/8703068 [Accessed: 25.11.2021]

Zaki, M., Sivakumar, V., Shirvastava S. & Gaurav, K. (2021) Cyberseurity Framework For Healthcare Industry Using NGFW. Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks. Available from: https://ieeexplore.ieee.org/abstract/document/9388455 [Accessed: 26.11.2021]