Compromising a Medical Mannequin case study discussion summary

Given that cyber threats rise exponentially and due to the inherently sensitive nature of the medical field, it becomes apparent that devices like pacemakers, insulin pump systems, cochlear devices, and many more are also vulnerable to cyber-attacks.

This case study has been a great example of cybersecurity risks in the medical industry and became a stimulus for further research leading me to conclude that the medical sector has overlooked the cybersecurity part despite the stringent safety and approval protocols applying on these devices.

Key points :

- Implant devices' size and capacity set some unavoidable limitations regarding the resources and the security technics that can be implemented. Therefore, cryptography and authentication parts should be considered diversely and more efficiently.
- A wired connection for the setup or for changing parameters is not an option in most cases. That is the most critical vulnerability, which was also presented in the case study.
- The most challenging part is the equilibrium between security and accessibility. It is vital to get the best from both worlds to ensure that the health personnel will have the necessary access in the shortest period in case of emergency.
- Some innovative and promising research paradigms could constitute a solid framework for medical devices' security.
- The intrinsic bureaucracy character of the Health Industry is also an obstacle that has to be taken into consideration while at the same time new cyber threats emerge constantly.

Final Thought: The Medical Industry seems that will suffer more from the cyber-crime perpetrators in the coming years. Medical IoT and implant devices could become hackers' playground, and the impact on human lives could be disastrous. This fact changes completely the priorities and the risks we have already faced. It is the human being under attack, and therefore the threat is upgraded to a whole different level.

Steve Morgan (2019), in his article "Patient Insecurity: Explosion Of The Internet Of Medical Things", cites some very stressful data, pointing out the magnitude of the problem in a very comprehensive way.

Reference:

Morgan, S., (2019) *Patient Insecurity: Explosion Of The Internet Of Medical Things*. Available from: https://cybersecurityventures.com/patient-insecurity-explosion-of-the-internet-of-medical-things/ [Accessed 23 June 2021].