**My collaborative discussions**

Healthcare Cyber Industries

Healthcare cybersecurity has become one of the significant threats in the healthcare industry. Unfortunately, many healthcare security vulnerabilities can compromise patients’ data. Without careful oversight, electronic health records as well as other valuable information can quickly fall into malicious hands.  When looking at potential threats, I consider: Brute force attacks and deniel-of-service;

Brute force attacks typically rely on weak passwords and careless network administration. Fortunately, these are both areas that can be improved easily in order to prevent vulnerabilities that could bring your network or website resources to their knees. For example, utilizing strong passwords, allowing a limited number of logins attempts and enabling two-factor authentication can help to prevent brute force attacks. Brute force attacks are usually used to obtain personal information such as passwords, passphrases, usernames and Personal Identification Numbers (PINS), and use a script, hacking application, or similar process to carry out a string of continuous attempts to get the information required.

Denial-of-Service Attacks: The goal of the DOS is to stop or hobble access to services or data on the target machine(s). Depending on the severity, this class of attack can be the domain of either the Vandal (who seeks to embarrass a victim) or the Soldier/Assassin if the service denied is critical to life support. Ransom-ware is an example of a DOS attack that uses cryptographic methods to deny access to data.

We may consider the following points as mitigation techniques

Educating Employees: Helping employees understand the role they play in cybersecurity and the impact it can have on patients’ lives fosters an atmosphere in which security is valued and respected. Regular briefings and communication on the state of the organization’s security reiterate the emphasis the organization is placing on cyber safety. Attending staff training sessions and making cybersecurity a regular topic in meetings could also help drive this message home.

Establishing Procedures**:**Create a plan that outlines specific protocols for dealing with information and networks both physical and virtual and make sure they are followed. By explicitly expressing the expectations, the process becomes standardized, allowing more comprehensive oversight for network security monitors.

Require Software Updates: Cybercriminals often take advantage of holes in outdated software or other unsecured access points. To combat this, force soft wear updates on machine, utilize two-factor authorization and automatically institute monthly password updates that require characteristics of a “strong” password. You can help your employees out with this by automatically setting company machines to periodically require such changes so that employees only have to come up with a new password or click to allow updates.

**References:**

1.    What is a Brute Force: Available in “ [**https://www.forcepoint.com/cyber-edu/brute-force-attack**](https://www.forcepoint.com/cyber-edu/brute-force-attack)” Accessed on May 12, 2012.

2.    Security Threats in HealthCare Systems: Available in “https://consoltech.com/blog/security-threats-healthcare-systems/”. Accessed on May 12, 2021

3.    Maydanchik A. (2007). BData Quality Assessment^, Technics Publications, LLC, Bradley Beach

4.    Top 10 Threats to Healthcare Security: Available in [**https://resources.infosecinstitute.com/topic/top-10-threats-healthcare-security/**](https://resources.infosecinstitute.com/topic/top-10-threats-healthcare-security/). Accessed on May 12, 2021

5.    Bel Air (2005). Open Web Application Security Project BOWASP Developers Guide V2.0

Use of CCTV data in a disciplinary process

This discussion was based on a case study concerns on unfair use of CCTV data in a disciplinary process regarding to processes, procedures, and the human element. As is often the case with such complaints, the complainant objected to the use of the CCTV footage as evidence in a disciplinary process that was taken by Air coach against her, the basis of the objection being that it was unfairly obtained. The law governing the processing of personal data, including CCTV images, is provided for under Section 2 of the Data Protection Acts 1988 and 2003. It is important to note that the processing of CCTV images in disciplinary proceedings against an employee is very much circumstance-dependent.

In addition to processes, procedures, and the human element Kin suggested the CCTV leakage also caused by the backdoors of these IoT. The latest MATT HANCOCK’s incident, has reported that his footage was recorded by the CCTV from China’s Hikvision. (BBC, 2021).

The leaking of CCTV’s data sometimes can be more complicated than other cyber security standards, such as DSS, HIPAA. It is because these incidents not only caused by human errors, but most of them are caused by backdoors which are set by the manufacturer.

So that the case shows that having processes, procedures, human element and regulation in place isn’t enough to use CCTV data or system in the organization. According to the IPVM (2017), we have to disclosed the backdoor of cameras. Also, it is worth considering how the data itself can be encoded as part of security precautions as well as looking at alternative mechanisms that may be usable.

References:

Unfair Use of CCTV Data. Available from: [**https://dataprotection.ie/en/pre-gdpr/case-studies**](https://dataprotection.ie/en/pre-gdpr/case-studies) [Accessed 26 June 2021].

BBC (2021) Newspaper headlines: Hancock hangs on - but is it a 'Barnard Castle moment?', Available at: https://www.bbc.co.uk/news/blogs-the-papers-57619698 [Accessed: 29th June 2021].