Network and Information Security Management May 2021 A

Home / / My courses/ / NISM_PCOM7E May 2021 A / / Unit 1 / / Collaborative Learning Discussion 1 /

/ Initial Post /

« Collaborative Learning Discussion 1

Yibeltal Mengesha

Initial Post

12 days ago

3 replies

Last 8 days ago

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**" 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/**. Accessed on May 12, 2021
5. Bel Air (2005). Open Web Application Security Project BOWASP Developers Guide V2.0.

Reply

3 replies

1

Post by **David Luvaha**

11 days ago

Peer Response

In support to the above the NHS Digital (2020) observes that utilizing medical hardware on clinical networks has three related issues: First, it is mandatory that security updates, patches and potentially virus signatures are accurately evaluated by the supplier and certified to be harmless prior to being deployed on the target medical hardware. Second, when security updates are released, they are retro-analysed by hackers, accumulating the probability that exploitable vulnerabilities will become recognized. Third, absence of latest security mitigations intensify the effect of vulnerabilities, creating favorable conditions for breaches occurring without detection. NHS Digital (2020) acknowledges that breaches related to security of connected medical hardware can cause substantial interruption to the service delivery in healthcare.

References

NHS Digital (2020) The problem with medical devices
Available from:
https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-medical-devices
[Accessed 13 May 2021].

Reply

2 Reply to David Luvaha from Jan Küfner ↑

8 days ago

peer response

I want to build on the point raised David Luvaha. Keeping your network up to date is crucial for a good defense. In some cases, this means, that you must replace hardware, since modern crypto algorithms might simply not be supported by the chips embedded in some older devices. In the scenario described by Glisson et. Al (2015) the router had outdated encryption (WPA) running, which can easily be bypassed. This is a picture-perfect example, that sometimes you need to invest in the latest technology, to not become a target for simple attacks.

References

Glisson, W., Andel, T., Mc Donald, J., Jacobs, M., Campbell, M. & Mayr, J. (2015) 'Compromising a Medical Mannequin', 21st Americas Conference on Information Systems. Fajardo, Puerto Rico, 13-15 August.

Reply

Maximum rating: -

3 Post by Kin Wong

10 days ago

Peer response

Besides technical issues, I think human factor is the highest potential risk of cyber security, which is also another possible factor under the scenario.

According to the Sky News today (2021) the IT systems of the Ireland’s health service are all being shut down because of significant ransomware attack, which maybe happened due to any human error.

According to Joseph (2021), he stated 5 network security risks which are happened by human error: The 1st one is allow the attacker connects to the network easily and physically, such as from any network plug, inside the hospital. It maybe an ethernet port on the back of the desktop hub, switch or router.

The 2nd one is the devices can be accessed by some 3rd parties. They can be medical device manufacturers, regulators, and so on. There is a risk for any 3rd party to access and attack the network.

The 3rd one is the hospital never expires any vulnerable devices, which may create security risk. For example, Windows XP and 7, which the Microsoft has stopped to provide any patch and service pack.

The 4th reason is the organisation’s policies and assessing compliance are not enough to defend the devices from being compromised, even though they all are compliant.

As the medical devices need to operate 24x7, the risk of data loss will be increased also.

References:

Sky News (2021) *Ireland's health service shuts down IT systems over 'significant ransomware attack',* Available at: https://news.sky.com/story/irelands-health-service-shuts-down-it-systems-over-significant-ransomware-attack-12305982 (Accessed: 14th May 2021).

Joseph, G (2021) *5 risks in protecting medical devices and how to meet them,* Available at: https://www.healthdatamanagement.com/list/5-risks-in-protecting-medical-devices-and-how-to-meet-them (Accessed: 14th May 2021).

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Paper - Compromising a Medical Mannequin

NEWER DISCUSSION

Initial Post