Network and Information Security Management May 2021 A

« Collaborative Learning Discussion 1

Dario De Giorgi

Initial Post

10 days ago

3 replies

Last 18 hours ago

The medical world is a sensitive environment, and protection against cyber-attacks must be implemented. Therefore, the security breaches in the article "compromising a medical Mannequin" is alarming.

In this post, I will highlight two security breaches detected during the brute force attack. To avoid undergoing such attacks, it is preferable to adopt some good practices, a solution to limit the attacks of type brute force, would be as the company Varonis mentions it, to deactivate the function "WPS" on the routers, given that WPS is used to recover the lost passwords, this tool will thus make it possible to give the complete access to the hacker, as shown in figure 8 in the reaver result.

Another piece of advice given by Varonis would be not to use a weak password for the wi-fi because the flaw of the WPA2 would allow using a brute force attack to find the password, it is also strongly advised to use a unique password for wi-fi access and not identical to the ID (Kinzie, N.D).

Kinzie, K. (N.D) Wi-Fi Security Tips: Avoid Being Easy Prey for Hackers. Available from : https://www.varonis.com/blog/7-wi-fi-security-tips-avoid-being-easy-prey-for-hackers/ [Accessed 14 May 2021].

Reply

3 replies

1 

Post by David Luvaha

10 days ago

Peer Response

In support of paragraph three above, NHS Digital (2020) says that it is of absolute necessity to regularly maintain User accounts. Every user who would like to carry out their daily tasks need to be registered in the system in a timely manner so that the system is available to them when they need it. User privileges need to be limited so that end users do not carry out tasks they shouldn't. User accounts must be maintained throughout the life cycle by deleting or disabling staff who left the organization

References

NHS Digital (2020) 3.6. User management
Available from:
https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/guidance-on-protecting-medical-devices
[Accessed 13 May 2021].

Reply

2 

Post by **Jan Küfner**

7 days ago

peer response

The mitigation as described in the initial post are good to prevent an attack to the medical mannequin as described in the article by Glisson et. al. (2015). Additionally, one should also switch to WPA2, since the used protocol (WPA) is outdated and can be easily attacked.

Since layered defense / defense in depth is a good technique to be secure from hacking attacks, further solutions should also be proposed to secure a network. Those solutions could for example be IP filtering (firewall, network segregation), update & patch management and an intrusion detection system (Ross 2008)

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.

Ross, A. (2008) Security Engineering: A Guide to Building Dependable Distributed Systems. Second Edition. Indianapolis: Wiley Publishing Inc.

Reply

Maximum rating: -

Post by **Dario De Giorgi**

3

18 hours ago

Summary post

Some good points were brought up by my classmates and several remedies were added to my initial post. There are several points that must be corrected when setting up a network for this type of sensitive data and then limit the risks of data breaches. We will review various good strategies to adopt in this use case in order to minimize the attacks. Since the beginning, it is strongly recommended to create a solid and robust network instead of fixing afterward when it's too late.

It is essential to disable the WPS if it is not used to avoid brute force attacks with the Reaver tool, as the 8 digits can be found in a few seconds if we have a laptop located next to the AP (CyberPunk, 2020) .

As mentioned by David, controlling who has access to the data is essential. Understanding who needs to have access to what, assigning correct rights to users without increasing their privileges if not required will cause problems for the hacker (National Cyber security centre, N.D).

As mentioned by Jan, setting up an IP packet filter can effectively deny traffic if the packets are not correct. IDS is also an essential tool as it allows to have several protections such as using valid signature identification, detect if there is a unusual presence on the network. IDS allows making a filter also on the protocols used on the network (Juniper, N.D).

In conclusion, it is necessary to implement good practices to protect against external attacks. It is not needed to spend a lot of money to protect against attacks. Setting up an unsecured network can cost more money and damage the credibility of the company in the event of an attack than if adequate protection had been put in place in the first place.

Reference :

Anon. (2020) Brute Force Attack Against WPS – Reaver. Available from: https://www.cyberpunk.rs/brute-force-attack-against-wps-reaver [Accessed 24 May 2021].

National Cyber Security Centre, (N.D) 10 Steps to Cyber Security. Available from : https://www.ncsc.gov.uk/collection/10-steps/identity-and-access-management [Accessed 24 May 2021].

IBM. (N.D) IP packet filter firewall. Available from : https://www.ibm.com/docs/en/i/7.1?topic=concepts-ip-packet-filter-firewall [Accessed 24 May 2021].

Juniper. (N.D) What is IDS and IPS? Available from : https://www.juniper.net/us/en/products-services/what-is/ids-ips/ [Accessed 24 May 2021].

Reply

Add your reply

Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

OLDER DISCUSSION

Initial Post