Destiny Hale

2/23/25

Medijacking

Numerous data breaches occur annually in healthcare facilities, leading to the loss of medical data due to outdated and unsecured systems. Since these systems cannot use cyber defense software, many healthcare facility devices and networks are highly vulnerable to malicious actors. In this write-up, I'll discuss a case study involving this issue, the nature of exposure and compromise, and mitigation strategies that healthcare facilities can use to prevent future cyberattacks.

Anatomy of a Medical Device Hacking

TrapX, a research lab company, performed four case studies to demonstrate how medical devices can be easily compromised and highlight the common security issues within them by creating a fake medical network. In the third case, they planted decoys within the virtual local area network to further analyze how malicious actors access the network and the process behind it. The systems that were used in the medical devices included older Windows software versions such as Windows XP, Windows 2003, Windows 2008, and Windows 2012. These software are commonly used in other organizations that use old versions of Windows and are most vulnerable to attacks. From a hacker's perspective, these are listed in payloads and common targets when exploiting. However, in this case study, the devices that had Windows XP and 2003 were affected by the malware while it ignored Windows 2008 and 2012 versions.

From the results of the case study, the malware targeted the PACS image viewer machine. The PACS system has access to medical records and patient images (TrapX Research Labs, 2018). Hackers can choose to leak, sell, or encrypt this information, violating the confidentiality of patients and affecting the availability of medical data. In the process, they also created a backdoor to establish a C&C with the image viewer. C&C stands for command and control. This is a technique that hackers use to communicate with compromised devices over a network (Palo Alto Networks). During operations, the hacker can interfere and tamper with the machine. The payload was able to avoid detection and scan for other networks, resulting in other devices being affected. The process continues with the malware copying the admin credentials to access the remote system to either reset, create tasks for the system to execute itself, or take control of the system. This case study demonstrates how fast a malware infection can spread and how it can compromise a system in seconds.

The Nature of Exposure and Compromise

Exposure occurs when a mistake gives the attacker indirect access to a system or network. This allows attackers to gather data or information from the exposed network or system (Tetrate, n.d.). Compromise is similar to exposure but involves infiltrating and manipulating the device via malware, viruses, or social engineering tactics (Reason Labs, n.d.). For example, case #3 perfectly demonstrated what exposure was, such as the outdated Windows software within the PACS image viewer machine. This enabled the hacker to infiltrate and compromise the system using a payload and take control. The nature of exposure and compromise is significant and crucial in maintaining great security measures. In healthcare facilities, this can be applied to recognizing vulnerabilities and understanding the impacts of a compromised medical device or

system. Assessing the values of each asset and recognizing the signs of what could be a vulnerability can shift the focus on protecting the critical areas of resources. Despite the FDA software restrictions, healthcare facilities can still protect themselves from cyberattacks with these principles. However, these two principles can be missed, sometimes unintentional, and vary depending on the damage.

Mitigation Strategies

Risk management plans, system and device monitoring, and security audits are a few mitigation strategies healthcare facilities can use to improve their security posture. Risk management plans help organizations identify, evaluate, and plan for potential risks (Hyperproof, n.d.). Hospitals and other urgent care facilities can use these plans to develop robust security policies, list assets and determine the value of each, estimate the costs of resources, etc. System and device monitoring can alert IT specialists of any suspicious activity within the network, device, or system. Additionally, this can help determine the severity of risks and what measures need to be taken to stay compliant with regulations to reduce them (Safety Culture, n.d.). Although these systems, software, and devices are outdated, they can still go under security audits. Identifying these vulnerabilities can allow healthcare facilities to effectively prioritize mitigation strategies and understand associated risks.

Conclusion

Numerous healthcare organizations are breached by hackers annually due to their outdated systems and devices, leading to a costly loss of medical data. A research company

called Trap X demonstrated this in four cases; however, the third case perfectly shows how these breaches can spread quickly and the nature of exposure and compromise. The nature of exposure and compromise is significant and crucial in maintaining a security posture. However, this can help these organizations understand the impacts of both and shift their focus on protecting critical areas to further prevent breaches and attacks. In addition to these two principles, mitigation strategies can effectively improve and strengthen the security posture.

References

Cybersecurity Risk Management: Frameworks, Plans, and Best Practices | Hyperproof

https://hyperproof.io/resource/cybersecurity-risk-management-process/

Medical Device Hijacking | TrapX Research Labs

https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf

What is a Command and Control Attack? | Palo Alto Networks

https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained

What is Compromised System? | Reason Labs

https://cyberpedia.reasonlabs.com/EN/compromised%20system.html

What Is a Cyber Exposure? | Tetrate

https://tetrate.io/faq/what-is-a-cybersecurity-exposure/

What is Risk Mitigation & Why is it Important? | Safety Culture

https://safetyculture.com/topics/risk-mitigation/