HealthManagement
Promoting Management and Leadership

Cybersecurity Challenges for Medical Imaging

Cybersecurity issues have been affecting the healthcare sector in recent years. As the use of the internet has expanded over the last two decades, hospitals worldwide have also adopted technology. Patient health information and electronic health records are now used routinely in healthcare.

However, while this adoption of technology is a positive for the healthcare industry, there has also been a dramatic increase in cybersecurity incidents such as computer virus, ransomware, theft and publication of patient data. In the past, most of these attacks were widespread and random, but several cyberattacks in 2019 were specifically aimed at medical network protocols and file formats, in particular digital imaging.

According to Nippon Telegraph and Telephone Security's 2017 Global Threat Intelligence Report, healthcare is among the sectors most affected by ransomware attacks. Here is a quick overview of cybersecurity challenges from the perspective of medical imaging and picture archiving and communications systems (PACS). Each scenario is described, and consequences and measures that could prevent the attacks from succeeding are discussed:

Scenario 1: Import of patient data from storage media that contains malware

In this scenario, a malware infection is caused by the import of patient data from a storage medium that is brought by the patient. Medical images are often given to patients on a CD, and the patient can carry this CD to a hospital where they have a follow-up treatment planned. These images are imported into the local PACS infrastructure of the hospital. However, a virus in the computer used to create the patient CD could cause this file to be infected, and wherever this file is opened thereafter, the virus spreads. At this point, the malware could intercept the network traffic, identify logins and passwords allowing the server to be controlled by attackers. This could then lead to ransomware. Measures to prevent such a thing from happening are quite simple. Antivirus software should be used on the side of the person creating the CD to prevent the creation and distribution of an infected storage media in the first place. Also, the AutoRun feature should be disabled on the import CD. The import system should be regularly updated and should also have an antivirus installed. A firewall should also be used, limiting the damage that could be caused by malware infection.

Scenario 2: Cyberattacker hacks the hospital network

In this scenario, the cyberattacker manages to get access to a hospital's internal local area network, which allows the attacker to intercept and analyse the network traffic. This gives the attacker information about the network addresses and port numbers as well as allows them to capture patient names, demographic data and other important information. The attacker also can get unauthorised access to images and patient reports. Once the hacker has access to this patient information, they can abuse this illegally acquired information for their own goals. This type of attack can be prevented by implementing several layers of defense. The first layer should include physical safeguards and secure network architecture. Cabled network ports should not be located in rooms that may have access to unauthorised persons. Network plugs should also be secured. Only computers with media access control addresses should be permitted to connect to the network. Wireless networks should be operated in a secure configuration and should be reviewed and updated regularly. Firewalls and network segmentation should be used to make the system more secure.

Scenario 3: Malware embedded in images or reports

In this scenario, the patient brings images or a report stored on a storage medium. This contains malware, but this malware remains inactive until the images or reports are viewed. When a radiologist retrieves and displays these documents, the malware is executed in the PACS network. It gains read access to the whole PACS archive and can also overwrite part of this archive as part of a ransomware attack. This type of attack can be prevented by testing applications that read and display documents and images and to identify any vulnerabilities before use. Also, these documents should only be accepted from a limited number of known sources and should be accompanied by digital signatures that are embedded in the document to prove that no malicious manipulation has occurred.

Scenario 4: Manipulation of medical images

The use of machine learning and artificial intelligence has significantly increased in recent years. However, one negative consequence of machine learning is the creation of deep fakes - convincing forgeries of images or videos. In this type of attack, the attacker manipulates medical images and injects modified images into the clinical workflow. The goal of the attackers is to place a small gateway computer and compromise the software. Once the gateway computer is placed, it can intercept, analyse and forward all messages and images. It can also intercept other network communication such as logins and passwords. The system can then begin to render false information into the image, can add or remove lesions and can manipulate images and patient information. Preventive measures to prevent this type of attack should aim to prevent physical access to the modality and unauthorised access. Network plugs should be physically secured, and the network switch should be configured properly. The goal should be to make it difficult for the attacker to install a gateway.

Scenario 5: Network infiltration of malicious HL7 messages

HL7 version 2 messages are commonly used to ensure consistent information across systems such as Hospital Information Systems, Radiology Information Systems and PACS. HL7 messages are used to update patient information automatically across multiple systems. These updates can change fields like patient name, address, telephone number, and they can also request merging of two patient records into one if needed. However, the HL7 message system does not have any means to prevent misuse or manipulation of such messages. It is easy for an attacker to passively monitor HL7 network traffic and get access to patient information, admissions, orders, diagnoses, and lab results. Also, an attacker could even send HL7 messages or modify legitimate messages during transmission. This type of attack could be prevented by protecting the HL7 message exchange with TLS using a bidirectional certificate exchange. This will help prevent the passive interception of the HL7 message traffic and the infiltration of malicious messages. Additional protection could include the implementation of application logic that would identify unusual patterns of message communication and immediately raise the alarm if such a thing is identified.

Overall, there are a number of ways cyberattackers can breach the medical imaging/PACS system. It is important to implement security measures, not only specific to PACS but throughout the hospital systems.

Source: Academic Radiology

Image Credit: iStock

Published on : Mon, 19 Oct 2020