Last Updated : 18th Nov 2003
First Published : 14th Jan, 2004

Rethinking PACS Security:
The Unusual Suspects

By: Adam Chee W.S

Note: This article is also published at PACSweb

Mention the word security to PACS administrators, and their main areas of concern would usually be workstations and servers. What they may be overlooking, however, is the modality equipment connected to the PACS network.

With the growing demand to connect their equipment to customers' PACSs, modality vendors have adopted an open platform by developing computer-based modality equipment running on Microsoft Windows. While this solution allows for easy management of both patient and image data, it also brings with it the security threats that the typical PC faces when it is connected to a network: vulnerability to unauthorized intrusion and worm or virus attacks.

Administrators might believe they are protected since their PACS network is sitting behind a firewall. This is an incorrect assumption, because security threats should always be prevented from within as well as outside of the organization.

Most organizations have a policy against connecting external computers or laptops to their network because an infected computer or laptop may introduce a virus into the network. Similarly, when a modality vendor connects an evaluation unit to a PACS network, it may introduce a virus into that network.

If infected, computer-based modality equipment could potentially become a base of operations to launch attacks against other computers and computer-based modalities in the network. These attacks can consume enormous network resources and bring the PACS network down, even if all of a facility's servers, workstations, and other computer-based modalities are well protected.

Because PACS are also integrated into the hospital network, it is possible that the infection will spread to the entire hospital system as well. Can a facility afford to have its PACS shut down?

PREVENTION IS BETTER THAN CURE

Once a system is compromised, it can be difficult to restore it back to its original self. The process is time-consuming, labor-intensive, and expensive.

The general rule is that as long as any computer or computer-based equipment is going to be connected to your PACS network, make sure it is clean of any viruses or malicious software (malware). Such an inspection should include:

- Computer-based modality equipment meant for evaluation purposes
- Computers or laptops for diagnostic modality equipment
- Any other computer-based equipment

If possible, administrators should require vendors to sign a declaration form, which includes penalty clauses making them liable for all costs incurred if downtime occurs due to vendor negligence. Administrators need to remain in the loop for all other devices connected to the PACS network.

When purchasing new modality equipment, make sure the tender and maintenance contract covers the following:

- ensure that the latest patch/update for the operating system is tested and applied within x weeks of release
- ensure that the latest security patch pertaining to the operating system is tested and applied within x weeks of release

In a Microsoft Windows context, patches and updates are included in Service Packs, while security patches are included in Security Hotfix. It is not necessary to specify any particular operating system because computer-based modality equipment can run on Linux, among other operating systems.

DETECTION, REACTION, DISCUSSION

With good preventive measures in hand, the next step is to minimize any accidents that may occur. The network needs to be monitored continuously. Departments should develop a patch management strategy to ensure that the vendor diligently performs whatever patches and updates are needed.

Another useful tool in the monitoring process is the Microsoft Baseline Security Analyzer, which helps to identify which system does not have the latest security updates and service packs.

Despite all of your best efforts, things will go wrong someday. In the event that security is compromised, what should be done?

This is an important question to ask, because once a PACS network is infected by malware

like the W32.Blaster.Worm, it is inevitable that downtime will be required. It could be that only the infected modality equipment needs to be disconnected from the network. Regardless, the possible scenario should be discussed with management ahead of time, so the nature of the probable downtime is understood. It is better not to start the discussion regarding downtime strategy only when disaster strikes.

During the discussion with management, administrators may encounter some difficulty. Many non-IT managers and supporting biomedical engineers may not be as technically savvy when it comes to IT-related security issues. Nevertheless, it is critical to keep the discussion going until management understands the critical nature of this issue and how it would affect the department's daily work processes, including the possible resulting damage to the institution's reputation.

Contact

Media and all other Queries: media@binaryhealthcare.com

About BinaryHealthcare.com

BinaryHealthcare.com is a vendor-neutral knowledge management repository pertaining to selected IT topics, Healthcare Informatics and its relevant industries (Biomedical Engineering, Radiology, Health Informatics, Telemedicine etc.) for working Professionals, students and anyone who is interested in this unique profession.

For more information, visit www.binaryhealthcare.com