HealthManagement
Promoting Management and Leadership

Volume 1 / Issue 4 Winter 2006 - Cover Story

Ensuring the Security of Radiological Networks

Authors

Giacomo Luccichenti, *MD*

StaffNeuroradiologist

Dept of Radiology

IRCCS Fondation Santa Lucia

Rome, Italy

g.luccichenti@email.it

www.hsantalucia.it

NhanNgoDinh

Chief Technical Officer

Dilogix S.r.l.

Rome, Italy

nhan.ngodinh@dilogix.it

Giulio Evangelisti

SystemSecurityManager

Dilogix S.r.l.

Rome, Italy

giulio.evangelisti@dilogix.it

www.dilogix.it

FilippoCademartiri, *MD,PhD*

Staff Radiologist

Dept. of Radiology

Azienda Ospedaliero-Universitaria di Parma

Parma, Italy

filippocademartiri@hotmail.com

StefanoBastianello, *MD,PhD*

Professor of Neuroradiology

Dept. Of Neuroradiology

University of Pavia – IRCCS Fondazione C.Mondino

Pavia, Italy

Stefano.bastianello@unipv.it

www.mondino.it

Over the past decade, the development of networking systems has dramatically improved the management of patient information and, as a consequence, the radiological workflow. On the other hand, the accessibility to a patient's data and images puts confidential information at risk. Every person in a hospital is somehow involved in safekeeping this information: from the system architect during the building and planning stage, to the medical and non-medical personnel in putting the information after implementation.

Clearly, the in-depth knowledge of security criteria cannot be required from all of these people. However, it may be useful for them to be aware of general protection strategies, management and security issues involved in the access to patient information.

Network Security Issues

Because the structure of TCP/IP networks allows for the exchange of data between IP nodes that are interconnected, data can be carried not only directly, but also through other nodes. Therefore, the structure of TCP/IP networks exposes this information to several security problems:

• Sniffing: other people can see transmitted data that is flowing through the node they can have access to;

• IPhijacking: the Internet is a distributed network. In particular cases, this can allow a node to get the "IP identity" of another node;

• Denial of Service: software applications that are used to provide network services can be crashed if they receive a particular sequence of data. When such software crashes, the service can have problems or can even stop; and

• Hacking: with the same technique used for Denial of Service, the partial or the complete control of the device can be taken from the outside.

Guidelines

In implementing network and information security measures in a radiological network, the following guidelines should be employed:

1. Identify a computer specialist proficient in network security and legal issues;

2. Check the security (physical, behavioural, and network /software issues) with the computer specialist, following established security standards;

3. Define the radiological devices that will be used and the staff who need to access the network (and their corresponding access level);

4. Train people accessing the network on the organisation's standard security procedures; and

5. Plan a periodical security audit and a subsequent activity report.

Information Security Issues

Information security encompasses the safety measures for preserving information from damage, resulting from unsuitable, unwanted and illegal use. For the purpose of this article, we have identified three categories of security issuesnand what measures should be taken to protect information in each:

Physical Issues

• Areas where information is present must be protected from physical and chemical damage; and

• Access to places where information is produced, managed and stored must be restricted and recorded.

Behavioural Issues

• Personnel working in a hospital should be periodically trained on general concepts of security issues; and

• Standard Operating Procedures (SOPs) should be developed in order to avoid omissions, reduce errors and protect information from unwanted or illegal access.

Network and Software Issues

• Access to computers where information is produced, managed and stored must be restricted and recorded;

• SOPs for accessing information should be present; and

• The network (and the computers) must be controlled.

This list of topics may also be useful in verifying information security in a radiological department.

Security Solutions

Protect the Ordinary PC LAN

The ordinary PC network should be protected through the implementation of an appropriate firewall to protect the LAN from the WAN. However, a firewall isn't sufficient without the proper configuration appropriate to meet the security requirements and the accessibility of the network it is installed on.

Create a Separate Radiological LAN

Mission critical devices such as scanners, printers and radiological workstations may be positioned on a network that is physically separated from the network of the ordinary PCs, thus increasing performance and avoiding data sniffing from ordinary PCs. A firewall should control the interaction between the “radiological network” and the ordinary PC network to provide, if needed, accessibility to inner services.

Teleradiology Issues

Teleradiology systems are much more difficult to protect. As a general rule, any connection to the exterior of the LAN should be encrypted and access should be granted only after proper authentication has occurred.

If there is the need to share the services between the two distant LANs,aVirtual Private Network (VPN) can be established through the creation of an “encrypted tunnel”. The most common encryption protocols used in such transmissions are Secure Socket Layer (SSL) or Transport Layer Security (TLS).

Published on : Mon, 1 Jan 2007