HealthManagement.org
Promoting Management and Leadership

Common cybersecurity weak spots and how to tackle them

Maintaining the safety and protection of IT systems that keep important health information requires discipline. This is especially true in this era of the Internet of Things (Iot), when more and more eHealth devices and other gadgets get connected to a provider organisation's IT system or network. Thus, ensuring that these connected devices are secure is of utmost importance.

Often hackers look for easy access to poorly protected devices and clearly printers would be a good example. Because the "innocuous" printers are everywhere in an organisation, they are one of the easiest devices to become a door to ransom or steal data, according to infosec experts.

It must be noted that IoT manufacturers are focused more on the products they build rather than how secure they are, says Brian NeSmith, CEO at Artic Wolf Networks, which continuously monitors infrastructures and identifies data security threats under contract with a provider.

What makes it more challenging in today's IoT world is that the underlying technology of legacy systems often is Windows or Linux-based applications, such as medication administration systems and other medical devices that often are not well maintained.

Another weak spot can be security tools themselves. These applications often produce false positives of an attack, and over time, people get alert fatigue and don’t pay attention to alarms that suggest an incursion has occurred, and that opens the door to new dangers.

To prevent alert fatigue and further improve the safety of healthcare IT infrastructure, infosec experts suggest the following:

- A combination of machine learning technology and data security talent can go a long way toward improving the security environment. Machine learning uses predictive outcomes software that improves the more it is used, the experts explain.

- Hire a “security engineer” with advanced training and skills. NeSmith says these skills include understanding social engineering to deceive individuals into divulging sensitive data, and training employees into recognising when they are about to be fooled.

- Develop best practices for decreasing the time it takes to detect a breach. Unfortunately, NeSmith says, “the best practice often starts with a weekly look at logs, which later becomes once a month and then becomes

once every six weeks or more.”

Source: Health Data Management
Image Credit: Pixabay

Published on : Wed, 1 Nov 2017