HealthManagement
Promoting Management and Leadership

Volume 16 - Issue 3, 2016 - Cover Story

Medical Device Cybersecurity

ECRI Institute, Welwyn Garden City, UK
******@***ecri.org.uk
LinkedIn Twitter

WHEN WILL YOUR PACEMAKER BE HACKED ?

In 2013, the Washington Post (among other news outlets) reported that Vice President Dick Cheney's cardiac pacemaker had its wireless capabilities disabled when implanted in 2007 to eliminate any potential cyberintrusion threat (Peterson, 2013). This old headline, with the more recent U.S. Food and Drug Administration (FDA) cybersecurity alert that the Hospira Symbiq Infusion System was hacked in 2015 (U.S. Food and Drug Administration, 2015), has many hospital leaders wondering whether they have the risk of medical device cyberhacking under control. General consensus is they don't.

Many information technology (IT) leaders certainly have many cybersecurity risks under control: passwords are required, servers are secured behind locked doors, policy has been established if any protected health information is sent to a wrong e-mail address or hacked. However, these practices have largely been applied to network infrastructure and the electronic health record (EHR). A medical device, such as a vital signs monitor or an infusion pump, is a cybersecurity threat vector that probably has not been subjected to the same risk-mitigation scrutiny.

To start addressing these issues, FDA hosted a public workshop January 20 and 21, 2016, called "Moving Forward: Collaborative Approaches to Medical Device Cybersecurity" (U.S. Food and Drug Administration, 2016). The FDA, in collaboration with the National Health Information Sharing Analysis Centre, the U.S. Department of Health and Human Services, and the Department of Homeland Security, brought together diverse stakeholders to discuss complex challenges in medical device cybersecurity that affect the medical device ecosystem.

Know Where the Threats Lurk

As we know, medical devices are no longer just machines attached to or used by the patient. They are often connected to the EHR—either hardwired or wirelessly. A typical patient in a critical care unit could easily be connected to ten or more networked devices. While the information on the medical device may not be useful to a hacker, the medical device can be used as a conduit for accessing patient information in the EHR, like home address and social security number, which can be used to perpetrate identity theft or real theft in the patient's home while the patient is hospitalised. Potential threats in medical devices include the physiologic monitor that runs on an outdated operating system, the ventilator with a USB port, and usernames and passwords for the vendor's field service engineers and in-house technicians that are hard-coded. Other industries largely solved these types of issues years ago.

As a further example, in-house biomedical engineering technicians and vendor field-service engineers typically have administrative rights to access performance records and to apply service diagnostics. These are typically not a managed credential and at many hospitals are the same for everyone with this level of access to the device. What happens if a technician or field service engineer leaves the hospital or the vendor? The password leaves with the person, with no hospital policy or procedure to update the access codes. In its 2015 Cybersecurity Survey, the Healthcare Information and Management Systems Society (HIMSS) noted that user-access control security solutions were implemented in just 55 percent of responding hospitals and mobile device management tools and that access control lists were implemented in only 50 percent of respondents (Healthcare Information and Management Systems Society, 2015).

Also, at many hospitals, no clinical engineering or IT staff can tell you which medical devices connect to the EHR, how they connect, or what version of operating software is running on each device. Often, basic security information is nowhere to be found regarding medical devices used in patient care.

What to do

- Include clinical engineering, IT, and risk management staff when creating cybersecurity policies and procedures;
- Proactively assess medical device cybersecurity risks. Working with manufacturers as appropriate;
- Keep up with the latest updates and patches for operating systems and anti-malware software;
- Limit network access to medical devices through the use of a firewall or virtual LAN;
- Audit the log-in process to all medical devices to ensure that an access-control method is being followed;
- Set up a process to monitor and report on cybersecurity threats and events.

Include the Right Stakeholders to Create Policies and Procedures

In its Top 10 Health Technology Hazards for 2015, ECRI Institute recommended that a hospital or health system clinical engineering, risk management, and IT departments jointly take these steps to mitigate cybersecurity threats. Also, medical device security should be thoroughly vetted during the purchasing process of all medical devices and equipment, with a team that includes clinical engineering, IT, and risk management personnel to assess what the vendor has done regarding design and policies for patch and update management. One resource to aid in this process is the Manufacturer Disclosure Statement for Medical Device Security questionnaire developed by HIMSS and the American College of Clinical Engineering, and then standardised during a joint effort between HIMSS and the National Electrical Manufacturers Association. It provides medical device manufacturers with a means for disclosing to healthcare providers the security-related features of the medical devices they manufacture.

Published on : Thu, 25 Aug 2016