HealthManagement
Promoting Management and Leadership

Protecting medical devices from malware attacks

In today's interconnected environment, protecting healthcare IT systems against malware attacks seems to be an uphill task for infosec professionals. The recent spate of ransomware attacks (e.g., WannaCry) has made many infosec teams to be more aware of cybersecurity issues associated with the Internet of Things (IoT). But some IT experts see some obstacles preventing CIOs and CISOs from actually addressing these security issues.

For starters, the equipment itself is unfixable. Today’s medical devices tend to be older because of the cost and time involved in upgrading, the experts say. Some of this equipment cannot be patched and will have known and published security flaws.

“Next, the CIO or CISO may not have the budget or policies to replace the unfixable items or even have a process that would embed cybersecurity issues into the device procurement RFPs,” said Sara Jost, global healthcare lead at cybersecurity firm BlackBerry. “There is also the issue that their own staff may be unable to employ best practices that can safeguard the organisation from all the new cybersecurity issues that are coming to light.”

When it comes to updating the technology, there's also the problem of selecting the right platform. Because of competition, every tech vendor wants to become the de facto platform to which all other devices adhere.

“The larger ecosystems say they are ‘open’ standards, so everything can be interoperable, but there are also smaller ecosystem players that may not adhere to the same specs,” Jost explained. “C-level executives are worried about hanging their hat – and future technology plan – on a platform that doesn’t win. Think of the Beta versus VHS battle.”

Another serious issue is lifecycle management.

“Devices are purchased with the expectation they will last for years. However, as threats evolve, there is not always a vendor expectation to maintain these devices and provide patches,” said Ryan Spanier, director of research at Kudelski Security. Things get complicated as many of these devices cannot be taken down for regular maintenance. For example, a device keeping a patient alive won’t be taken offline just to apply the latest security patch, even if there is a known vulnerability being exploited.

To reduce the impact of a cybersecurity attack, Spanier says a healthcare organisation should ensure vendors are willing to support the devices for the planned lifetime of the system. Hospitals also need to have contingency plans in place if a device is vulnerable to an attack but cannot be patched. "You may need to take devices off of the network until they can be patched, or provide specific network-based controls to protect the systems until they can be patched, such as closing a vulnerable port,” Spanier said.

In addition, some devices leave the healthcare facility – attached to a patient, for instance – and only occasionally return for check-ups. Hospitals need a plan in place for updating these devices even when they are not connected to your network.

It's important for hospitals to allocate the necessary budget for IT to address these IoT security challenges. That’s particularly true in today’s climate where many infosec teams are being asked to do more with less.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 7 Nov 2017