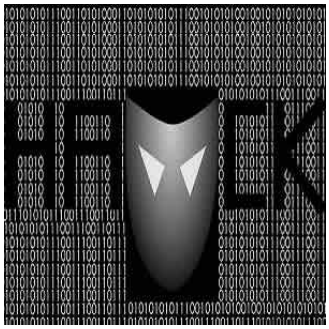
HealthManagement
Promoting Management and Leadership

HIT Hacking: Prevention is Better than Cure



By implementing cybersecurity best practices, healthcare CIOs and CISOs not only can thwart attacks on their IT systems but also make these less appealing targets for hackers, according to information security experts.

David Nickelson, director of strategy and behaviour at Sapient Health, says these three tactics can help hospital security teams stay one step ahead of cyberattackers:

Device cybersecurity. Hospital IT teams should build device cybersecurity into the procurement process. This involves talking to vendors and setting expectations about vulnerabilities, taking ISO's 2014 guidelines into account and preparing for the new ones due in 2019, as well as incorporating those into your own policies and procedures, explains Nickelson.

Cyber-hygiene. Make this a requirement when implementing guidelines for using medical devices, especially portable ones. Citing a HIMSS survey from 2016 that found only 56 percent of hospitals actively deploy protocols for medical device management, Nickelson said that "IT managers must think like care providers: Preventing an infection is better than treating one."

Risk management. IT teams should be able to assess risk and patch vulnerabilities in their systems. In late 2016, Nickelson pointed out, the FDA provided specific direction about how to address an identified cybersecurity risk across the entire health IT ecosystem without alarming patients and providers or tipping off would-be hackers interested in exploiting a known vulnerability. The guideline states that manufacturers can reach back and fix security issues without having to resubmit a device for recertification. "Prior to this explicit guidance, many manufacturers were reluctant to make changes that could be seen as fundamental alteration, which could trigger the need for recertification," he says.

In addition, Kate Kuehn of the BT Group also suggests these best practices like keeping firewalls up to date, training employees not to click on suspicious emails, and making sure to protect the right resources.

"The first thing we recommend is an in-depth understanding of your assets; while that seems obvious, what we find is more than half of the companies we work with actually are protecting the wrong things," Kuehn said.

An organisation needs to be aware of its perimeter to have an all-around defence. "From a borderless standpoint, what is a device on the network, what connects in, what about supply chain IT, what are you doing with mobile devices – have a really deep understanding and doing an annual assessment of what is connecting to see where that shadow IT is," Kuehn emphasised. "Printers now carry a lot of personal data. Cameras are being used for attacks.

Every organisation has some kind of experience with cybersecurity. All these things we are talking about concern a disciplined security practice, according to Kuehn. "And especially in healthcare, whenever you can take the offensive rather than the defensive, you become less appealing to attackers."

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Tue, 20 Jun 2017