HealthManagement
Promoting Management and Leadership

The Internet of Things and On-line Security

The Internet of Things (IoT) means all sorts of devices we use today, be it at home or in the workplace, are practically linked/connected to each other or to a network. While such connectivity leads to improved efficiency in what we do (eg, smartphones for fast communication), security experts warn that the IoT puts these connected devices at risk of being hacked.

You may also like: Do you do these 7 things to get C-suite behind cybersecurity?

Indeed, who would have thought that a device as simple as a fish tank thermometer could be used as an entry point to launch a ransomware attack on a casino? It's frightening to think if such an attack targets medical devices and equipment, which play a crucial role in saving people's lives.

Not surprisingly, hospitals are now being more careful when purchasing medical devices especially amidst reports that even pacemakers and infusion pumps may be vulnerable to cybersecurity attacks. However, as noted by tech expert Mike Kijewski, even if a device has been approved by the Food and Drug Administration (FDA), this is not a guarantee that it is 100% secure.

You may also like: Patient Trust Needed for Healthcare Data Security

In 2016, for example, a security researcher found vulnerabilities in St. Jude Medical pacemakers, prompting the FDA and Homeland Security to issue an alert for about 465,000 pacemakers from St. Jude, an Abbott-owned company. The FDA alert was accompanied by a firmware update to close the security flaw of the radio frequency communication devices. In addition, in 2017, implantable cardioverter defibrillators and cardiac resynchronisation, also made by St. Jude, were recalled from the market upon FDA's order "due to premature battery depletion."

"The biggest areas now of concern are medical devices," Cheryl Martin, chief knowledge officer for the American Health Information Management Association, points out, adding that with the IoT "everything is just a small computer now." Martin warns the next target is just about anything that plugs in and is wireless, including printers, phones, as well as Alexa, Siri and Google Assistant.

A hospital contains numerous connected devices, and interoperability entails the secure sharing of sensitive health data. It should be noted that HIPAA compliance mandates hospitals secure protected health information.

"Medical device security is a big, important problem," according to Kijewski who is the CEO at MedCrypt, a company that builds security features into medical devices. With rising concerns about security of medical gadgets, the FDA has issued guidelines on strengthening the agency's medical device programme to protect patients, adds Kijewski.

Furthermore, in coordination with the MITRE Corporation, the FDA announced the launch of a cybersecurity "playbook" to help healthcare provider organisations boost their cybersecurity readiness. The FDA's premarket guidance also mandates that manufacturers, in designing and developing their medical device, should ensure their product adequately addresses cybersecurity vulnerabilities.

Meanwhile, the agency's postmarket guidance provides a risk-based framework for manufacturers to use to ensure they could quickly and adequately respond to new cybersecurity threats once a device is in use.

Source: Healthcare Finance

Published on : Tue, 3 Sep 2019