HealthManagement
Promoting Management and Leadership

Ransomware Seen as Medical Device Cybersecurity Threat

As adoption of Internet of Things (IoT) technology increases, there's growing concern about the security and safety of networked medical devices. A U.S. Department of Homeland Security official has warned that medical devices are increasingly targeted by ransomware attacks.

When it comes to “ransomware moving into the embedded device” area, it’s not a matter of “if” but “when” given that the “proof-of-concept code is already in existence for that,” according to Marty Edwards, director of the Department of Homeland Security’s Industrial Control Systems Cyber Emergency Response Team. As such, he believes that this could be the year that medical devices get hit with the equivalent of the malicious computer worm Stuxnet, which damaged Iran’s nuclear programme.

At the recent RSA Conference in San Francisco, there was wide discussion around the probability of ransomware transitioning from the healthcare IT environment, where it is now, to the clinical environment. When that kind of cyberattack moves into the operating room, for example, doctors won't be able to use the machinery that they need as it’s held ransom for so many bitcoins, Edwards explained.

As early as September 2015, the Federal Bureau of Investigation issued an alert warning about the cybersecurity risks that networked medical devices pose to patients. According to the FBI, IoT devices — which connect to the web automatically sending or receiving data, including medical devices such as wireless heart monitors and insulin dispensers — pose a potential threat to patient health as hackers could change the coding controlling the dispensing of medicines.

“By connecting into the Internet, we’ve actually created a threat surface that has ballooned,” said Denise Anderson, president of the National Health Information Sharing and Analysis Center, a non-profit organisation dedicated to protecting the health sector from physical and cyber attacks and incidents.

Edwards also noted that the healthcare industry does not have the “device-based instrumentation to even be able to log some of these security events in these environments.”

Source: Health Data Management
Image Credit: Pixabay

Published on : Tue, 28 Feb 2017