HealthManagement
Promoting Management and Leadership

WannaCry Attack Highlights Concerns on Cybersecurity

The recent massive cyberattack that infected more than 200,000 computers in 150 countries, including hospitals in Britain, highlights the importance of updating and securing health IT systems. The malware, known as "WannaCry," paralysed computers running banks, factories, government agencies, transport systems and hospital emergency services.

In the U.S., one legislator noted that the largest cyberattack to date highlighted the acute concerns around cybersecurity, particularly for hospitals.

“This is big: around the world, doctors and nurses are scrambling to treat patients without their digital records or prescription dosages, ambulances are being rerouted, and millions of people’s data is potentially exposed,” Sen. Ben Sasse, R-Neb., said in a statement. “Cybersecurity isn’t a hypothetical problem – today shows it can be life or death. We’ll likely look back at this as a watershed moment.”

Rob Wainwright, director of Europol, the European Union’s law enforcement agency, said that the WannaCry attack is “unprecedented in scale” and told British journalist Robert Peston that the attack “sends a very clear message that all sectors are vulnerable.” He urged NHS to follow the example of the financial industry that has invested in cybersecurity.

In the aftermath of WannaCry attack, NHS hospitals were forced to divert patients from the emergency room and cancel scheduled surgeries. NHS Digital was offering 24/7 support to hospitals affected by the attack, noting that the “vast majority of NHS organisations” are running contemporary systems. Three days after the cyberattack, NHS Barts Health, which operates four hospitals in London, continued to “experience IT disruption” and had reduced the volume of planned services.

According to Britain's defence secretary, Michael Fallon, the NHS was repeatedly warned about cyberthreats and was given £50 million to update its systems.

After indicating that it had seen “evidence” of ransomware attacks, the U.S. Department of Health and Human Services issued an update warning providers that attackers were scanning the internet for Remote Desktop Protocol (RDP) servers as an entry point for the malware.

“Once connected, an attacker can try to guess passwords for users on the system, or look for backdoors giving them access,” HHS said in an emailed statement. “Once in, it is just like they are logged onto the system from a monitor and keyboard.”

Source: Fierce Healthcare
Image Credit: NHS

Published on : Tue, 16 May 2017

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.