HealthManagement
Promoting Management and Leadership

Ransomware on the Rise; EHRs Prime Targets

Cyberattacks on hospital IT systems are likely to continue, with security experts warning that 2017 could be even worse than last year for the healthcare industry. The reason: more hackers recognise the value in rich medical record data. Stolen patient health records can fetch as much as $60 per record.

See Also: ‘No More Ransom’ Grows: Thousands of Users Get Hacked Data Without Paying

In particular, a surge in ransomware attacks is predicted this year. Ransomware is a type of malware that blocks access to a patient's records until ransom is paid. There is growing talk that 2017 will also be the year of the first ransomworm which will help spread various flavours of ransomware even faster, like crypto-ransomware that encrypts files.

In 2016, there have been approximately 4,000 ransomware attacks per day, compared to the preceding year's 1,000 attacks per day, according to a recent U.S. Government report. It is estimated that the average ransom will be $300,000 per day, a staggering increase from today’s payment of about 2 Bitcoins or $670 daily.

EHRs as Primary Targets?

According to IT security experts, hospital system EHRs are likely to be cyberattackers’ prime targets given that access to EHRs has become more mobile with tablets and smartphones. This makes it easy for data hackers to bypass perimeter security, enabling cyber thieves to pose as authorised users with access to hospital networks for unlimited periods of time. Medical staff and other employees need to be more aware about data protection, and an easy way to do this is to remind them not to click on suspicious links.

With hackers getting more sophisticated with their methods, providers may be able to thwart their malicious with the help of healthcare IT consultants versed in solutions like security defences leveraging the skyrocketing AI boom. With cloud-based resources and AI, consultants have the core building blocks to launch a bold, comprehensive defence strategy.

The security team's primary goal is to safeguard the EHR data; protecting the network or the perimeter is secondary. "If your data is protected, the roads leading to it become less strategic. Why have post-incident responses when you can deploy a pre-incident response? It is the old stop chasing the rats and protect the cheese argument," says Santosh Varughese, president of Cognetyx, a developer of advanced AI security solutions.

"A data centric approach can also mitigate the argument of whether threats are caused more by rogue insiders or malicious outsiders. It simply will not matter," Varughese points out. "The real solution for medical facilities in 2017 is to concentrate IT security efforts on protecting the data by deploying an AI strategy using forensic technology. IDC forecasts global spending on cognitive systems will reach nearly $31.3 billion in 2019."

Source: HIT Consultant Media

Image Credit: Pixabay

Published on : Tue, 17 Jan 2017