HealthManagement
Promoting Management and Leadership

4 Steps for Fighting Ransomware

Researchers have supported cybersecurity guidelines put forward by The National Institute of Standards and Technology (NIST) in a paper published in Applied Clinical Informatics.
Dean Sittig professor at the University of Texas School of Biomedical Informatics and Hardeep Singh, MD. Chief of Veterans Affairs Health Policy, Quality and Informatics Programme say that CIOs and CISOs understand that user training is one aspect of cybersecurity healthcare management should not overlook.
data. Another critical aspect not to overlook, of course, is user training.
"While preventing all ransomware attacks is not possible, there are a number of steps healthcare organisations can take to reduce their risk as well as mitigate potential harm," they say.
The researchers' strategy is four-pronged and prevention focused. Based on the framework of the NIST, Sittig and Singh propose the following steps to secure EHRs and protecting underlying computing infrastructure:

Step 1:
Keep security protection in mind when configuring computers and networks

Backup data and update software regularly;
Create system-wide data backup processes and keep programmes up to date with latest patches. This includes operating systems, applications, browsers, plug-ins, firmware and anti-virus tools;
Keep a 'white list' of software programmes that users are permitted to run and another list f those that risk carrying malicious code that staff are prohibited to use.

See Also: Meet Latest Ransomware: Crysis

Step 2:
Put user-focused strategies in place to ensure reliability of defence systems

Train users for secure operation of apps and devices;
Teach staff how to identity potentially malicious emails;
Conduct regular phishing attacks in order to educate employees;
Conduct regular risk and impact assessments in order to prioritise applications which can undergo downtime and, in the event of an attack, for how long.

Step 3: Monitor suspicious activity thoroughly

Use systems for surveillance of suspicious activity. These could include receipt of email messages from notorious sources or a noticeable and unexpected rise in traffic.

Step 4: Respond, recover, investigate, and track lessons learned

In the event of an attack, shut down computers and networks immediately;
When the threat is contained, contact the insurance provider a computer forensics expert and the FBI's Internet Crime Complaint Centre;
Following the attack, IT professionals and clinicians should meet to try to identify the root of the attack in order to prevent a recurrence;
"Similar to approaches to address other complex socio-technical health IT challenges, the responsibility of preventing, mitigating, and recovering from these attacks is shared between health IT professionals and end-users," said Sittig and Singh wrote.

Source: HealthcareITNews
Image Credit: Pixabay

Published on : Tue, 26 Jul 2016