What can Small Healthcare Providers Do To Prevent Ransomware Attacks?

Posted by HIPAA Journal on Mar 23, 2017

Ransomware attacks on healthcare providers are occurring with alarming frequency. Figures from the FBI suggest as many as 4,000 ransomware attacks are occurring every day.

Healthcare organizations are targeted because they hold large volumes of data and access to those data is required to provide medical services to patients. Without access to patients' health information, healthcare services can be severely disrupted. Such reliance on data makes healthcare providers attractive targets as they are more likely than other companies to give in to ransom demands to obtain keys to unlock their data.

All businesses, and healthcare organizations especially, should implement a number of defenses to prevent ransomware attacks. Policies and procedures should also be developed to ensure that in the event of an attack, business operations are not severely disrupted and data can be recovered quickly.

There is no one technology solution that can be deployed to prevent ransomware attacks from occurring, although there are a number of actions that can be taken to improve resilience against ransomware attacks and ensure a fast recovery can be made at minimal cost.

How to Prevent Ransomware Attacks

Listed below are some of the steps that healthcare providers should take to improve their defenses against ransomware.

- Deploy and configure an anti-spam solution – Consider all of the email attachments that are likely to be required by employees and block all others, especially JavaScript (JS) and Visual Basic (VBS) files, executables (.exe), screensaver files (SCR)
- Configure computers to display file extensions. Double extensions are often used to trick end users to believing files are harmless. Invoice.xlsx.scr for example. Displaying file extensions will help users to identify malicious files.
- Ensure Office installations are configured to block macros, or at least ensure macros must be run manually. Make sure all employees are warned of the dangers of enabling and running macros.
- Ransomware infections often occur via Windows PowerShell. Unless PowerShell is essential, consider disabling it
- Ensure all software is kept up to date and patches are applied promptly
- Segment your network – An attack on one device should not allow all of the company's data to be encrypted
- Provide training to all employees on security best practices and instruct them never to open email attachment – or visit links – contained in emails from unknown senders
- Consider an Internet filtering solution that can be used to block end users from visiting malicious websites

- Ensure anti-virus software is installed and virus definitions are set to update automatically. Consider installing a popup blocker in web browsers.
- Block all unused ports on computers
- Train all staff members on basic cybersecurity and best practices
- Conduct dummy phishing email tests to ensure training has been effective
- Ensure all employees are trained on the correct response to a potential attack. Ensure staff members are made aware of the importance of reporting any suspicious emails and how to respond if they believe they may have inadvertently installed ransomware
- Ensure that policies and procedures are developed that can be instantly implemented in the event of an attack. Fast reaction can limit the harm caused and will ensure the fastest possible recovery from attack
- Consider encrypting data. While this will not prevent a ransomware attack, if an attack does occur and encrypted data are encrypted by ransomware, patient notifications will not need to be issued and a breach report will not need to be submitted to Office for Civil Rights.

Most important of all is to ensure data are backed up daily. Backups should be stored securely in the cloud. Local backups should be stored on air-gapped devices. Backup drives should not be left connected after backups have been performed. Backup drives can also be encrypted by ransomware.

Reporting Ransomware Attacks and Notifying Patients

HIPAA Rules require ransomware attacks to be reported if the protected health information of patients has been accessed or encrypted, unless the covered entity can demonstrate there was a low probability that patient data were compromised in an attack.

While some healthcare organizations have disclosed ransomware attacks, many are not reporting the incidents. The failure to report a ransomware attack and notify patients that their ePHI has been compromised can potentially result in financial penalties for noncompliance with HIPAA Rules.

To avoid a HIPAA penalty, a covered entity must be able to demonstrate there was a low probability of patient data being accessed or copied during an attack. The Department of Health and Human Services' Office for Civil Rights released guidance for covered entities on ransomware infections last year. In the guidance, covered entities are advised of the steps that should be taken following a ransomware attack and the criteria for determining whether patient notifications must be issued.