Ransomware: What to Do When Your Systems are Hijacked

Electronic healthcare security systems were put to the test in 2016, as record numbers of hospitals, facilities and physician practices fell victim to ransomware attacks. The increasing number of ransomware attacks on providers is particularly troublesome because hackers can essentially lock out users from their EHR systems. Once a system is infected, providers feel compelled to pay the ransom rather than sustaining an interruption to patient care. For these reasons, providers should learn about the risks of ransomware and develop strategies to prevent and manage such malicious cyber-attacks.

Ransomware refers to malicious software that attempts to deny access to a user's data, usually by encrypting the data in a way that prohibits access until a ransom is paid. Computer systems affected by ransomware will see ominous messages, indicating that their computer is essentially locked out, except for a web-link that directs the user to pay a ransom to a hacker. The ransom is usually demanded in Bitcoin or other cryptocurrency and requires the user to access the "dark web" to make the payment. Hackers promise that upon payment they will release a decryption key, which will restore the user's system. However, there have been instances where hackers do not honor their promises and instead demand more money.

> In addition to the general problems created by ransomware, healthcare businesses must also consider their obligations under HIPAA and other privacy and security laws. According to guidance from the Department of Health and Human Services (HHS), the presence of ransomware is a "security incident" under the HIPAA Security Rule and triggers the security incident and response and reporting procedures required under HIPAA.

HHS guidance also states that any electronic protected health information ("ePHI") that is encrypted by ransomware is presumed a "breach," triggering a covered entity's breach notification obligations. Although ransomware does not typically distribute or disclose computer files that are held hostage, HHS states that the act of taking possession or control of ePHI by unauthorized individuals constitutes a breach. HIPAA's breach notification rules can seriously compromise the goodwill and reputation of a provider, as notification to affected individuals, to the Secretary of HHS and to the media (for breaches affecting over 500 individuals) may be required. The breach notification obligations can only be avoided if the victim of a ransomware attack can demonstrate that there is a "…low probability that the PHI has been compromised," based on the factors set forth in the breach notification rules.

Preventing ransomware is a complex undertaking, as this particular strain of malware is constantly evolving and infiltrating even those systems that follow recommended security measures. HHS guidance recommends that providers follow the HIPAA security rule to prevent ransomware infections. In particular, providers should implement a robust and frequent data backup plan, which would enable providers to restore previous “infection-free” versions of their electronic data. Providers should also invest in reputable security software (e.g., firewalls, e-mail filters, anti-virus programs) and promptly install updates, which periodically update the software’s ability to recognize and detect new ransomware attacks.

Once a ransomware attack is identified and underway, providers are encouraged to follow a security incident response plan. According to HHS guidance, this includes conducting an initial analysis, that determines the scope of the attack (what systems were affected?), the origination of the incident, whether the incident is ongoing, finished or spread further throughout a network, nd analysis of how the incident occurred. Thereafter, appropriate response activities include containing the infection and preventing propagation of the malware, eradicating instances of ransomware, recover from the ransomware attack by restoring data or backups and conducting post-incident activities that address identified vulnerabilities.

Providers should also consider reporting the attack to its local FBI or U.S. Secret Service field office. These agencies work with Federal, state, local and international partners to pursue cyber criminals globally and assist victims of cybercrime. The FBI has also released guidance to help victims of ransomware attacks, which echoes the recommendations set forth in the HHS guidance.

Physician practices that wish to avoid ransomware attacks should implement robust security incident response protocols. These protocols should include education and training that helps members of the workforce to identify, prevent and address ransomware attacks.

Yulian Shtern, Esq., is a health law attorney with Abrams, Fensterman, Fensterman, Eisman, Formato, Ferrara & Wolf, LLP.

See Related

Read More

“When Your Patient Asks for Medical Marijuana” in Physician’s Practice

06/28/2016

Read More