Prevent Your Company's Data from Being the Next Ransomware Hostage!

Insights
3.02.16

A few weeks ago Los Angeles-based hospital Hollywood Presbyterian Medical Center fell victim to cyber criminals who infiltrated and disabled the hospital's computer network through the use of ransomware. The malware reportedly locked access to certain computer systems and prevented hospital staff from sharing communications electronically.

The hospital opted to pay the ransom in the form of 40 Bitcoins, equivalent to approximately $17,000. According to Hospital President and CEO Allen Stefanek, complying with the demands of the hackers was the quickest and most efficient way to restore the hospital's systems and administrative functions. "In the best interest of restoring normal operations, we did this", said Stefanek.

This incident should be a wake-up call for any organization that stores and uses critical information. Ransomware is a growing trend in cyber attacks and no business is immune. Cybersecurity firm Bromium reports that thousands of Internet users have fallen victim to ransomware attacks, while thousands more go unreported. According to Bromium, victims may experience anxiety or disbelief and "are likely to paythe ransom to end the incident, often without reporting the crime in order toavoid further embarrassment."

So What Is Ransomware?
Ransomware is a type of malicious software (malware) that infects a computer and restricts access to it until a ransom is paid to unlock it. Ransomware is typically spread through downloading attachments in phishing e-mails and visiting infected websites. Crypto ransomware, a variant that encrypts files, has also been spread through Web-based instant messaging applications.

How Do I Protect My Business from Ransomware?
First and foremost, regularly back-up critical information. Data should be kept on separate devices that are stored offline. If you properly back-up data, you may avoid the question of "to pay or not to pay" altogether.

1. Maintain up-to-date anti-virus software; install pop-up blockers and ad-blocking software.
2. Train your employees on how to avoid social engineering and phishing attacks. See the Department of Homeland Security's security tips**:** https://www.us-cert.gov/ncas/tips/ST04-

014Develop protocols on reporting and responding to data security incidents.

3. Invest in or review the scope of your cyber insurance coverage. Many insurers offer coverage for "cyber extortion," which may cover ransom payments.

Every business, no matter the industry, should take steps to prevent their data from being taken hostage by cyber criminals.

Related People

Melissa A. Dials
Partner
440.740.2108
Email