Ransomware Attack Highlights Importance of Preparation

Authors: Alisa L. Chestler, Samuel Lanier Felker
February 19, 2016

Hollywood Presbyterian Medical Center in Los Angeles recently paid a $17,000 ransom in bitcoins to a malware hacker who seized control of the hospital's computer systems and demanded money ransom as a condition to returning access, the hospital's chief executive said. The cyber-attack occurred February 5, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices. The malware locked key systems by encrypting files, rendering them unusable by staff. Without the decryption key from the hackers, the hospital had no access to its own systems. According to the CEO, "[t]he quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key." The hospital said it alerted authorities and was able to restore its computer systems with the assistance of technology experts, but the episode lasted ten days. Reports currently indicate there was no evidence that any patient or employee information was subject to unauthorized access. However, the event disrupted operations and forced the hospital to return to pen and paper for its record-keeping.

This leaves all organizations with the question – what should we do to protect ourselves? Here are a few high level suggestions:

1. Be ready for a ransomware attack by having a plan in place. Make sure your company's documented Data Incident Policy and Procedure is current and contains the information needed to respond effectively and quickly. It should include details regarding who employees are to contact – day or night – including the emergency phone numbers and email addresses for critical team members, federal authorities and outside vendors such as technical forensic investigators and experienced breach-response legal counsel. Include decision trees for potential events including a ransomware attack, a distributed denial-of-service (DDoS) attack or a breach of personal information. While it appears the hospital was able to quickly react and turn off the systems to reduce the potential for a breach of personal information, would your organization be able to do the same as quickly?

2. Organizations must test their policies and procedures to ensure that they are appropriate and that all executives understand the implications of the decisions made. We strongly recommend a "bench test" exercise of your Data Incident Policy and Procedure to make sure the plan works for your organization and that employees understand the policies and procedures well enough to respond appropriately. Don't wait until trouble strikes.

3. Ensure the organization's security program includes a detailed disaster recovery and business continuity program (DR/BC Program). These DR/BC Programs are not limited to planning for situations such as fires, earthquakes, floods and hurricanes – they should include the potential for a ransomware or DDoS attack. Organizations should have a good understanding of the latency for back up files and the ability to switch to another hot site or third party location. The recovery points and objectives for the recovery should be known in advance. Important data should be backed up regularly and saved via unconnected storage solutions. When data is backed up appropriately, ransomware demands become less effective.

4. All organizations must continue to update operating system and security software on a regular and consistent basis. Investing in the right tools and protocols can be costly, however those costs should be evaluated with the new paradigm in mind – one in which your organization could be rendered paralyzed at the whim of a criminal.

5. Have a good understanding of information governance and its role in your comprehensive security program. Unfortunately, we have worked with clients who have a security program in place, but one that is missing key and critical pieces that could have been identified easily with a small investment in the development of an information governance program. Be vigilant and you will be ready if your organization is the next target of a malicious malware ransom attack.

For more information on how this issue may affect your business or related matters, contact Alisa Chestler, CIPP/US and Sam Felker, or any members of Baker Donelson's Privacy and Information Security Team.