Ransomware Attack

Are You Prepared?

Ransomware is a type of malicious software (malware) that infects your information Systems and denies you access to your data by encrypting it, so you cannot access it. To obtain the decryption key, the cyber criminals demand a ransom payment. Cyber criminals have attacked all sizes of organizations from large to small so don't make the mistake to think that a ransomware attack cannot occur to your organization. On average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. The most common method cyber criminals deliver their malware to your organization is through emails and their attachments, or your staff downloading software from unknown websites. Let's look at how you can prepare your organization against a ransomware attack from two perspectives; prevention and recovery. The following are recommendations and best practices provided by the United States Government.

Your first and obvious goal is to prevent the ransomware attack in the first place. While there are technical steps you must take to prevent the malware, the human factor plays a very large role as well. Staff education is your best defense. You should have a robust training program that educates your staff about ransomware and how to prevent and detect it. You should complement the training program with technical preventive measures.

- Implement an awareness and training program
  - Train staff to identify anomalies and malicious software
  - Train staff not to open unknown e-mails with attachments
  - Train staff to recognize the inability to access certain files as a possible ransomware attack
- Test restoration of data on a periodic basis to ensure it is working
- Implement vulnerability patching through a "patch management" program
- Conduct periodic (annual) penetration testing to identify security holes in your systems
- Enable strong spam filters to prevent phishing emails from reaching the end user
- Enable anti-virus and anti-malware programs to run regular scans automatically
- Configure firewalls to block access to known malicious IP addresses
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransom locations
- Maintain frequent backups of critical operational data (your PHI)
- Maintain backups physically offline or in the cloud so they're not connected to the network

Despite your best efforts, you may still fall victim to ransomware. When this occurs, you should be prepared to respond at the first sign of a ransomware attack and activate your security incident response team and plan. This is the same team you would activate for any other type of security incident, to include activating your business continuity plan if needed.

The security incident response team should consider the following steps:

- Determine the scope of the incident to identify what networks, systems, or applications are affected
- Determine the origin of the incident (who/what/where/when)
- Determine whether the incident is finished, is ongoing, or has propagated additional incidents throughout the information systems
- Determine how the incident occurred (tools and attack methods used, vulnerabilities exploited, etc.)

Once you have determined you have a ransomware incident in progress, you should consider the following steps:

- Isolate the infected computer immediately
  - Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives
- Isolate or power-off affected devices that have not yet been completely corrupted
  - This may afford more time to clean and recover data, contain damage, and prevent worsening conditions
- Immediately secure backup data or systems by taking them offline
  - Ensure backups are free of malware as you will depend on the backups to restore operations

Continued on page 2…

Ransomware Attack continued…

- Contact law enforcement immediately
  - Contact your local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service to request assistance with your ransomware incident
- If possible, change all account/network passwords after removing the system from the network
  - In addition, once the malware is removed from the system, change all system passwords

Activating your business continuity plan simply means taking required steps to continue business operations. While your data is encrypted & not available to you because of the ransomware, your response efforts should be to "restore the data" from your clean backups. It is easy to understand why it is imperative that you have a good data backup program, which is also a required implementation specification under the HIPAA security rule. Having viable data backup *can eliminate you having to pay ransom* so you can return to normal operating conditions as soon as possible. Whether you pay the ransom or not will be based on your ability to restore your data & advice from the FBI/Secret Service. There have been instances where the organization has paid the ransom, yet the criminal hackers did not provide the decryption key. Paying the ransom is clearly a leadership decision.

The year 2017 saw several major ransomware attacks that made the news, and the attacks continue today:

- The *NotPetya* ransomware attack started as a fake Ukrainian tax software update & went on to infect hundreds of thousands of computers in more than 100 countries over the course of just a few days.
- *WannaCry* has been one of the most devastating ransomware attacks in history, affecting several hundred thousand machines & crippling banks, law enforcement agencies, and other infrastructure.
- *Spora* ransomware is distributed when cybercriminals hack legitimate websites and add JavaScript code, making a pop-up alert appear that prompts users to update their Chrome browsers. Upon infection, the ransomware can steal credentials from victims, making money from both extorting ransoms and potentially selling the stolen information.
- *Cryptomix* is one of the few types of ransomware that does not have a type of payment portal available on the dark web. Instead, victims must wait for the cybercriminals who locked their machine to email them instructions for payment in Bitcoin.
- Jigsaw, first seen in 2016, embeds an image of the clown from the Saw movies into a spam email. When the user clicks it, the ransomware encrypts their files, but also deletes files if the user takes too long to make the ransom payment of $150, according to Webroot.

Ransomware is a crippling security incident that no organization wants to experience. Implementing preventive measures and training your staff is your best defense. After recovering from a ransomware incident, you must also assess if you have a HIPAA breach under the privacy rule which is beyond the scope of this article. Please review https://www.hhs.gov/hipaa/for-professionals/index.html for further guidance on breach reporting.

The following are federal government resources that can help you in the invent of a ransomware attack:

Federal Bureau of Investigation:
Cyber Task Forces: www.fbi.gov/contact-us/field
Internet Crime Complaint Center: www.ic3.gov

United States Secret Service:
Local Field Offices: www.secretservice.gov/contact/

Mitigation:
Dept. of Homeland Security United States Computer Emergency Readiness Team (US-CERT): www.us-cert.gov

Information for this article was sourced from the US Government Interagency Technical Guidance document, the Ransomware & HIPAA fact sheet from HHS, and article "Top 10 Ransomware Attacks for 2017", by Alison Raymone from TechRepublic.

Hernan Serrano
HIPAAtrek
www.HIPAAtrek.com