Ransomware: A Looming Threat To Title Agents

Description

We have all heard about Ransomware, but what exactly is it?

Ransomware is a form of malicious software (malware) designed to deny access to systems and/or encrypt files on a device rendering any files and the systems that rely on them unusable.

Unfortunately, cybercriminals understand how lucrative real estate information is, making an attack not a matter of if, but when.

So, how does it work?

Ransomware attacks are extremely complex and meticulously engineered to penetrate networks, but to sum it up in a nutshell it can be broken into five parts:

1. **Infection**: The malicious email/website has exploited the vulnerability in your network.
2. **Execution**: The malware targets your title production software, client management applications, document management systems, email etc. and downloads all the information into their network.
3. **Encryption**: Your systems and files are locked using a unique encryption key held by the perpetrator.

4. **Demand**: The company receives a ransom notice with a demand in exchange for the key to decrypt and regain access to their network and files.

5. **Payment**: A payment, usually in cryptocurrency, is made in exchange for the decryption key that will reinstate access to your network, devices and applications.

What is the possible impact of ransomware?

Logging in and receiving the notice that your network has been compromised is a living nightmare. Not only is your title production software, document management systems, and communication networks inaccessible, but there are implications if you donâ??t pay the ransom including:

- Temporary or permanent loss of sensitive or proprietary information, disruption to regular operations,
- Financial losses incurred to restore systems and files, and potential harm to an organizationâ??s reputation.
- Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victimâ??s money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.
- Inability to pay the ransom results in the release or sale of all your business and clientsâ?? information.

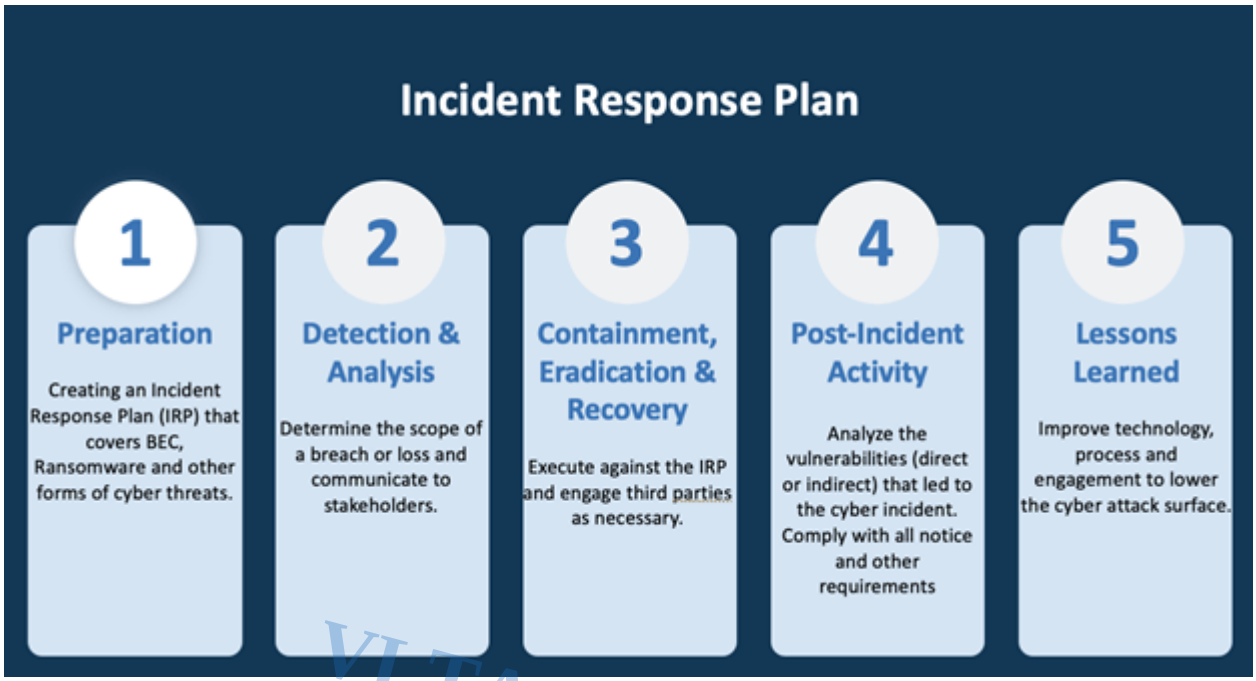
How do I lower my risk of a ransomware attack?

Here are a few strategies to protect your data and network from a ransomware attack:

- **Updates**: Keep operating systems, software, devices, applications up to date with the newest versions
- **Antivirus:** Enable antivirus and anti-malware scanning tools with automatic updates and regular scan sequence
- **Backups:** Regular and co-located backups with confirmation of completion
- **Emails:** Scan all incoming and outgoing emails to detect and prevent threats. Train employees to detect and report suspicious emails, links, and attachments.
- **Whitelisting:** Restrict access to unwanted and high-risk sites, content, and applications

What if itâ??s too late?

If a breach occurs itâ??s essential to have an incident response (IRP) that covers ransomware, business email compromise (BEC), and other forms of cyber threats. The response will vary on the type of breach, company size, and severity of the attack, but this is an excellent start to begin formulation of your plan:



Here are two great resources about ransomware and how to prepare for a ransomware attack.

U.S. Secret Service â?? Ransomware Preparation Guide:

Click to access Preparing%20for%20a%20Cyber%20Incident%20-%20A%20Guide%20to%20Ransomware%20v%201.0.pdf

CyberSecurity & Infrastructure Security Agency:

Click to access CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

Authored by Tom Cronkright (Co-Founder) and Nick Lock (Customer Success Manager) of CertifID. For more information visit: http://www.certifid.com or email: support@certifid.com

Category

1. Cybersecurity

2. Uncategorized

Date Created
2021/09/30
Author
vltaexaminer