ONE REALLY GOOD IDEA EVERY DAY
attorneyatwork@™

Protect Your Law Firm from Ransomware Attacks

BY JOE KELLY | ATTORNEY AT WORK DAILY DISPATCH

May 11, 2016

It's 6 p.m. You are about to put the final touches on a brief that is due tomorrow when a message pops up on your laptop. It informs you that a third party has gained control of your system and encrypted all your files. To unencrypt your files, you must pay a ransom.

Every single file you have on your computer system is now unreadable. Thanks to this ransomware attack, your practice has basically been shut down while your system is held hostage.

What Is Ransomware?

Ransomware is a type of malevolent program that limits the functionality of victims' computers. For example, it could disable your computer altogether, encrypt your files so you can't read them or bar applications like Word or a web browser from working. Ransomware attacks have grown exponentially in number in the past few years.

The most common methods of becoming infected include unknowingly via a download (clicking on an infected site, ad or email that prompts an illicit download of the malware) or via program weaknesses (an outdated operating system, for example). After the ransomware is downloaded, generally only a unique "key" can decrypt the victim's files.

Ransom amounts vary, but the price — depending on the hacker behind the scheme — is usually about $500. Larger corporations may face significantly higher ransoms. Often the message will imply that you have been using your computer illegally and must pay a government fine as a punishment. The hackers normally demand payment in bitcoins, a digital form of currency that is difficult to track.

Ransomware is big business for hackers. According to McAfee, there were more than 4 million samples of ransomware in the second quarter of 2015. Those instances are expected to grow in 2016. The FBI estimates that the Cryptowall program alone accrued over $18 million by June 2015.

Responding to Ransomware

Many ransomware programs are extremely difficult to combat — that is what hackers count on. However, there are some steps you can take to work around a virus, rather than simply paying off hackers.

One way is to recover files. The easiest way to fix a virus is to clean it off the infected properties and restore the information from backup systems. That is why you should frequently back up your files and use a service that provides redundant backup facilities.

When a firm has the option of paying hackers a lot of money or losing a couple of minutes of work and restoring from files that have been backed up, the choice becomes obvious. If you are not completely satisfied with your backup system and provider, now is a good time to conduct a review and make any necessary changes.

Not all hackers are criminals. Some white-hat hackers work to provide keys that can break ransomware encryptions. You can send these white hats your infected files to be analyzed by experts. Then, they provide the key to unlock the files, typically free of charge.

Law firms can also use file-accessing auditing to open their files. This functionality, which is built into Microsoft Windows and available through most secure, cloud-based solutions, tracks each time a user opens a file or folder. By monitoring the logging activity, the firm's IT professionals can identify patterns or instances of unauthorized access. Through file-accessing auditing, you can launch a course of action such as stopping the server or removing file share so that you can halt the attack.

Avoiding Ransomware Attacks

Of course, the most effective approach to fighting ransomware is avoiding attacks in the first place — by using both technological and human approaches.

Technological approaches involve having an extremely robust spam-filtering service that will automatically block certain file types that may transmit viruses. You should also use pop-up blockers and always keep your software up to date so hackers cannot access servers through older, vulnerable software.

Also, consider storing your data in the cloud instead of directly on the hard drives of laptops, computers and smartphones. This can give you another, more sophisticated level of protection for your information — assuming you've done your due diligence on your cloud provider. While a laptop may be infected, the files in the cloud will remain safe.

Firms should work with IT and security professionals to ensure that all administrative access and levels are securely locked down and that only a small number of authorized users have advanced privileges. A ransomware virus potentially has access to every single program that an individual user's device does. By ensuring that your staff and attorneys only have permissions to access the information they absolutely must have, critical files and systems can remain cordoned off from many potential attacks.

You should also promote awareness of the dangers of ransomware among your firm's attorneys and staff through frequent updates and training so that everyone knows what ransomware is, how it can infect systems and the best security practices to follow to prevent it.

Finally, you must always back up your data to ensure that you will have updated backup files to replace infected ones.

While law firms have been hearing for years that they could be the victims of a cyberattack, the danger has never been clearer. In the past two months alone, the media has reported investigations into cyberattacks on several major law firms (where hackers may have been looking for information to use for insider trading) as well as the leaking of the Panama Papers from Mossack Fonseca.

Law firms hold some of their clients' most important trade secrets, corporate data and sensitive information about potential deals and are being actively targeted by hackers. In this environment, every firm needs to understand the risks ransomware attacks pose and take steps to minimize them.

Joe Kelly *formally launched Legal Workspace in 2010 and leads the organization as the CEO. He also founded Denver-based Business Network Consulting, Ltd., recognized by Inc. magazine as one of the fastest-growing companies in the nation for five consecutive years. Splitting his time between Dallas and Denver, Joe is a passionate entrepreneur who is constantly looking to leverage technology to make it easier for law firms and other organizations to do business.*