THE NAVIGATOR
COMPASS
NETWORK GROUP

September 2016

4 Signs You're a Victim of Ransomware

Ransomware, although it may invoke images of kidnapping and ransom notes, looks rather different in the PC world, and – it's not always so obvious.

For example, when ransomware affects a server and the storage connected to it, "the remote user trying to access the shared volume will not have seen the ransom note and the files will no longer open up properly. It will look like corruption to the users and until the system admin looks at the server to see the ransom note all users can be chasing their tails."

In a recent CSO Online interview, Mike Cobb from DriveSavers identified signs of ransomware.

Here are four signs Cobb says you should look for to see if you might be a victim of ransomware:

1. A Splash Screen Blocks Access

When you startup your computer and you see a splash screen with instructions on how to pay the ransom to restore access – it's the most obvious sign that you're infected with **lock screen ransomware.**

2. Files Will Not Open

If you cannot open individual files on your computer and receive an error message specific to Windows or Mac, you might be a victim of **encryption ransomware.**

3. Odd or Missing File Extensions

While common file extensions include .doc, .exe, .pdf and .jpeg., files that are encrypted by ransomware often have extensions that end with something like .crypted or .cryptor, or, they are missing file extensions altogether.

4. Instructions for Paying the Ransom

If your computer has been infected with ransomware, you'll receive payment instructions by the hacker.

The files should be quite easy to locate on your computer - look for .txt or .html files that begin with an underscore (_) followed by clear language in all caps, such as "_ OPEN ME", "_DECRYPT YOUR FILES".

CALL COMPASS IMMEDIATELY: The longer you wait the higher the potential for lost data and downtime.

CLICK HERE TO READ MORE

10 Easy Ways to Prevent Malware Infection

There's a lot of talk about how to tell if you're infected with malware, and how to clean up the infected computer. Unfortunately, the damage from some forms of malware, like ransomware, cannot be undone. If your files have been encrypted and you haven't backed them up, it's looking really bad.

While there isn't a 100 percent proven method, there certainly are some cybersecurity techniques for keeping malware infections away.

So, let's take a look at how to prevent the malware infection:

1. Be diligent about updating your operating system, browsers, and plugins

2. Enable click-to-play plugins

3. Remove software you don't use

4. Be careful with the emails you receive

5. Do not call fake tech support numbers

6. Practice safe browsing

7. Use strong passwords and/or password managers

8. Make sure you're on a secure connection

9. Log out of websites after you're done

10. Use firewall, antivirus, anti-malware, and anti-exploit technology.

Security professionals agree a multi-layer security - using not only multiple layers of security technology but also user awareness – will help prevent malware.

Contact Compass today to help you manage many of the items listed above - (866) 336-8727

Ransomware Could Cost You Millions of Dollars

Did you know that cybercriminals are profiting almost $35 million a year by targeting individuals and businesses with ransomware?

A new security report from Cisco Systems Inc. showed that more than 9,500 people pay ransoms to hackers each month.

CryptoWall is one of the most persistent forms of ransomware, which encrypts a user's files, and demands a ransom to be paid to responsible hackers to make them accessible again.

Its newest version, CryptoWall 3, was reported by the Cyber Threat Alliance as being responsible for 406,887 attempted infections and approximately $325 million in damages in the last year or so. According to the report, "Of the roughly 70,000 instances where CW3 has been seen, about two-thirds of these have been via phishing email".

It was also indicated that computer devices with outdated software are left at the mercy of hackers who could gain access into corporate networks.

Cisco security researchers also revealed a large surge in HTTPS traffic related to malicious activity between September 2015 and March 2016, mostly due to malicious ad injectors and adware.

Businesses looking to prevent these types of attacks can seek different solutions, including creating and testing an incident response plan and being vigilant about trusting HTTPS connections and SSL certificates, as well as educating employees about the threat of malicious browser infections.

Don't let Ransomware derail your business. Contact Compass today.

Are You Protecting
Your Patients' Medical Records from Ransomware?

Patient records are sought-after more than ever, their black market value continues to grow, and the attempts to illegally obtain them are on the rise.

In recent months, hospitals and health systems have increasingly been targeted by cybercriminals and made victims of ransomware, and the ramifications can be devastating.

Millions of stolen medical records worldwide are up for sale online. Some healthcare organizations have ended up paying thousands of dollars to retrieve their patients' medical records. Unfortunately, ransomware is only one of many ways your sensitive data is at risk.

Hackers are now starting to use personal information not only for identity theft, but also to blackmail patients for money.

41 Action News revealed at least 159 million patient records had been breached in the past. There are thousands of health care providers that have been investigated since the HIPAA privacy rule began in 2003.

The federal government reported that, over the last seven years only, at least 159,000,000 patients had their medical records breached, and many were targeted online. Data breaches continue to happen, even after health care providers were fined more than $36,000,000 by the federal government for failing to secure patient information.

The challenge is - patients may not even notice the threat right away. So the risk of the hack comes many years later, and the impact can last forever.

Legal advisors recommend that health care providers ensure they encrypt their patients' medical information, train staff on privacy laws, and use a layered security approach to allow only the doctor to see patients' personal information.

Let Compass help you protect your patients' information.
Contact us today: (866) 336-8727

SERVICE HIGHLIGHT: HIPAA Compliance

HIPAA Enforcement Rule

The HIPAA Enforcement Rule governs the investigations that follow a breach of ePHI, the penalties that could be imposed on covered entities responsible for an avoidable breach of ePHI and the procedures for hearings.

Although not part of a HIPAA compliance checklist, covered entities should be aware of the following penalties:

- A violation attributable to ignorance can attract a fine of $100 – $50,000.
- A violation which occurred despite reasonable vigilance can attract a fine of $1,000 – $50,000.
- A violation due to willful neglect which is corrected within thirty days will attract a fine of between $10,000 and $50,000.
- A violation due to willful neglect which is not corrected within thirty days will attract the maximum fine of $50,000.

Fines are imposed per violation category and reflect the number of records exposed in a breach and risk posed by the exposure of that data. Penalties can easily reach the maximum fine of $1,500,000 per year, per violation category. It should also be noted that the penalties for willful neglect can also lead to criminal charges being filed. Civil lawsuits for damages can also be filed by victims of a breach.

Protect Your Practice with Compass.

Our team will lead you to HIPAA compliance through comprehensive IT solutions.

No Stress. No Hassle.
No Problems.

CLICK HERE to take Our Survey Today To See How Compliant You Are

