RESPONSE | THE MAGAZINE FOR MEDIA, TECHNOLOGY & COMMERCE

Technology

Guest Opinion: Understanding and Preventing a Ransomware Attack

by *Matti Kon* | Dec 1, 2017 12:00am

On a day-to-day basis, you hear about computer systems and cybersecurity, and — more so — you hear about bridging and violating the cyberworld and cybersecurity. In fact, this year more than $80 billion will be invested in dealing with cybersecurity and information systems.

Almost every day, a breaking news report comes out about various cybersecurity threats: Russians hacked the Democratic National Committee during the 2016 presidential election; a hospital had the medical records of its patients stolen and held ransom; financial companies had their confidential information held ransom; records were stolen from the IRS; and credit companies had sensitive information of their clients compromised.

These are just a few examples — there were thousands of other violations and cybersecurity threats causing damage and distraction.

The field of cybercrime is as big and complicated as any science out there — if not more. There are different types of crimes, different technologies used to perform crimes, different agendas, and different targets. In the words of targeted cybercrime, the famous quote, “Different strokes for different folks,” is implemented to perfection.

One of the most common cybercrimes is performed using something called ransomware. This type of malware is a form of malicious code that infiltrates your computer, network, or system through email links, attachments, or other vulnerabilities and proceeds to encrypt each and every file on that computer without prejudice.

The ransomware will then prompt you with a screen with instructions on how to unlock your files, which normally requires you to pay a price within an allotted time. The best analogy for ransomware is “bullying.” It is the kid that we all remember from kindergarten that comes into your sandbox, looks at the beautiful sandcastle that you built and says, “Unless you give me your lunch, I will destroy your castle.”

The number of businesses that did not protect themselves properly in advance from such a scenario is innumerable. These businesses are held ransom with a short time to make payments to the cyber criminals. Without doing so, they risk compromising their data, which forces everyone to pay the ransom.

More than 70 percent of companies hit by ransomware attacks find themselves out of business within six months. The ramifications of the snowball effect in the period that follows a cybersecurity incident are usually much more than the businesses can predict or foresee.

Leading business solutions and cybersecurity companies will make it their duty to implement a variety of cybersecurity policies and procedures. Some of these procedures include implementing day-to-day monitoring of any potential cybersecurity violations and educational training for employees. Improper employee behavior on computer systems causes a majority of all cybersecurity violations and makes it easy for criminals to exploit the systems' data.

If your business hasn't done so already, it must subscribe to some form of service or consulting firm to help protect your it, its system integrity, and its cybersecurity footprint.

Read more on Guest Opinion, InfoTech Solutions, Matti Kon

About the Author

Matti Kon

✉