Stand Up to Ransomware with Cloud Backup

June 23 2016

Imagine you are an IT administrator at a small company of 30 people or so. You juggle hardware, software, the network – and even phone systems and the occasional electrical failure or power outage on any given day. So, when your CEO calls you and says, “I cannot open my sales forecast file,” you rush into action. You check your CEO’s PC and find that the file is somehow corrupted. Then you notice a small red icon at the bottom corner of the desktop with a prompt reading: “Your files have been encrypted. Pay $500 for a decryption key within 10 days or your data will be deleted — click here for payment instructions.”

After the initial shock, you realize that you have been infected by *Ransomware* – a type of malware that blocks access to files or your systems until the ransom is paid. There are many types of Ransomware, including Reveton, Cryptolocker, Winlocker, and Cryptowall, and for many the antidote may not be available yet. According to McAfee Labs Threats Report (March 2016), each quarter the number of new Ransomware reach in average 40,000,000 of new malicious

hashes discovered. Moreover, the threat of Mobile Malware is increasing especially since the last quarter (reaching 13 Million new malware).

What Would You Do?

Think about what you would do if Ransomware hits your company. Would you pay? Unless you can find an antidote out there – you may have no way to restore your data. Remember, even if you did pay, there is no guarantee that the attacker would decrypt your data and not just disappear.

However, what may come as a surprise to you is that the universal solution against Ransomware has existed for years. In fact, it has existed even longer than Ransomware itself:

It's called **Backup**!

Now, some things have changed since backup first came onto the scene years ago. Today, cloud backup is the best way to protect your data and systems from Ransomware – and more and more companies can take advantage of it through local service providers, hosts, and resellers.

Cloud backup creates copies of all your files, and even your entire operating system – and keeps it safe, away from attackers and the threats of Ransomware. If an attack happens, you can quickly restore the affected files and keep your business up and running. You can even restore an entire system to the previous, clean state – and you would not need to pay a penny in ransom.

Note that traditional local backup may not be sufficient – as the backup files on your local USB HDD or NAS can also be affected by Ransomware.

The only ultimate way to stand up to Ransomware is to use professional-grade data protection solution to back up your data and systems to the cloud on a regular, consistent schedule.

SafeComs Backup Service can help protect your entire environment from Ransomware. By using Cloud Backup solution, your data will be safe and accessible at any time. For more security, we can as well encrypt your data.

Read more about our backup solutions here.

Source: http://www.acronis.com/en-au/blog/posts/stand-ransomware-cloud-backup