How to Avoid Being a Victim of Ransomware: 5 Top Tips

Introduction

Our last blog reviewed what Ransomware is, how it is deployed, and the various types of attacks which can occur. Essentially, it is a type of Cyber-attack that can literally lock up your computer screen, all of your mission critical files, and even the data that your company depends upon on a daily basis.

The only way that you can ever hope to recover your files is if you pay a ransom to the Cyber attacker. But, here is the tricky part. Simply paying in hard currency is not enough. It has to be in a Crypto currency like Bitcoin. The reason for this is that by paying up with a virtual currency, the tracks of the Cyber attacker cannot be detected as easily if marked currency was actually used.

In this blog, we look at some of the ways as to how you can protect your business from a Ransomware attack.

The Top 5 Tips

1) Always back up your data:

   This should be a no brainer, and in fact it is one of the oldest mantras in the word of Cyber security. There are various methods in which how you can back your data. For instance, you can have both an on premises and off premises solution. In fact, depending upon the size of your data and files, it is recommended that you have both. With the former, it is highly recommended that you keep this backup in a different physical location, and with the latter, using the Cloud is the prime choice. Equally important is to make sure that you back up all of your mission critical files on at least a daily basis, if not more. So, if you ever do become a victim of a Ransomware attack, all you have to do is just procure another computing device(s) and restore your files from backup.

2) Do not open up any suspicious links or attachments in your E-Mail:

   Believe it or not, sending out a Phishing E-Mail is still one of the most favored techniques of the Cyber attacker. Therefore, as it has always been said, ***do not click on any suspicious links or open any kind or type of E-Mail attachment*** that you are not expecting to receive. Be especially careful of those file extensions that end with .DOC, .PPT, and .XLS. In this regard, it is also important to keep in mind, that a Cyber attacker will very often use the name and E-Mail address from an individual in your electronic address book, in an attempt to make the fake E-Mail look legitimate. If you receive an E-Mail like this (in other words, not expecting it), always contact the sender to confirm if he or she has actually sent this E-Mail or not. If they did not, ***delete it immediately***!!! This is also goes for those pop-up messages that appear in your web browser. They often make use of scare tactics so that you will be tempted to click onto the link that is embedded into them. Very often, these links contain the Ransomware .EXE files which will very quickly find their way into your computer if clicked on.

3) Always keep your computer updated:

   It is always important to keep your servers, computers, and even your wireless devices up to date with the latest software patches and upgrades. True, it may be a pain sometimes doing

this (especially if you have the Windows 10 OS), but doing so will pay huge dividends in the end. Apart from this, there are also other preventative measures that you can take, which include the following:

*Always keep your Adobe Flash Player, and other Java based Web browsers up to date as well. This will help to prevent any kind of "Exploit Kit" Ransomware attacks from occurring.

*Disable the VSSADMIN.exe file:

This is an obscure file in the Windows OS in order to administer what is known as the "Volume Shadow Copy Service". This is used to keep a version history of files in your computer that are not used very often, or that are deemed to be arbitrary in nature. Since very few people actually use this tool, it has thus become a favored avenue of the Cyber attacker.

*Disable the other automated services in the Windows OS. These include the following:

→Script Host;

→Power Shell;

→Auto Play;

→Remote Services.

4) Shut down your entire computer system(s):

If you think you may be in the beginning stages of a Ransomware attack, immediately unplug your computer. This action will help to mitigate the actual .EXE file from entering into your computer. However, if your IT infrastructure is large, shutting down the entire system is still your best bet. True, this will cause some downtime, inconvenience, and lost revenue, ***but this cost is minimal*** when compared if your business or corporation were to be become an actual victim of a Ransomware attack.

5) Never, ever pay the Cyber attacker:

If in the unfortunate case that you do become a victim, ***never pay the Cyber attacker under any circumstances***. There are two primary reasons for this:

*Even if you do pay the ransom, there is no guarantee that you will get the decryption key in which to unlock your computer and files;

*Paying the Cyber attacker will only fuel their motivation and greed to launch more Ransomware attacks.

Conclusions

Finally, in the end, remember that you do not need all of the latest Security technologies to keep your business safe from a Ransomware attack. It just takes following the tried and true techniques as detailed in this blog. But, these are very often not enacted upon, so thus, these are the prime areas in which the Cyber attacker looks for in launching their next Ransomware attack.