RANSOMWARE – WOULD YOUR BUSINESS SURVIVE IF INFECTED?

Ransomware is a form of malware (or virus) that from a single point of penetration, quickly will infect your entire network and render your business **inoperable** unless resolved. It can arrive bundled as a treat with another malicious program, like a trojan, password-stealer, downloader, etc. It can arrive and infect on its own accord as well. Usual infection points are an email attachment, and there are new variants of the virus being released all the time. The virus may arrive in a zip file; when unzipped, an .EXE installs itself within the Operating System.

Once the virus is opened, it immediately begins to execute some tasks. Here are the tasks that Ransomware or Cryptolocker will execute.

1) The virus begins spreading to any mapped drives on the computer. If you open This PC (Windows 10) or My Computer (Windows 7), and on the left hand side where you have C: , D: etc. A mapped drive could be a folder anywhere on the network. Ransomware will start to encrypt local files on the local computer and all files on all mapped drives as well. It will spread to anywhere on the network that is mapped.
2) Because of this, any USB or thumb drive attached would also be affected.
3) Ransomware / Cryptolocker will attempt to spread itself over RDP ports that are left open.
4) Cryptolocker will target commonly used file extensions – Word files, Excel spreadsheets, Powerpoint presentations, PDF files, pictures (JPG, GIF, etc.)

How do I secure my network against Cryptovirus – Prevention Techniques

Cryptolocker is often not a virus that can be defeated, removed or “cured.” Once infected, you’re in for a wild ride. Thus, it’s extremely important to safeguard your network, servers, workstations and storage by utilizing some (or all) of the following methods:

1) Use a cloud backup service that does not use mapped network drives.
2) Use e-mail filtering services, that can filter out .exe and .zip files. Zip and EXE files are how viruses are attached to e-mails. Your staff open them, they execute and infect the local machine. They then infect the network. An e-mail filter service will flag incoming e-mails with these attachments, and potentially stop them from hitting the mailboxes of your staff
3) Disable files running from Windows AppData & LocalAppData folders. Policies, or rules within Windows can be created to disallow executables from AppData or Local App Data folders. Cryptlocker & Ransomware use these Windows directories to run the executable from.
4) Disable RDP on systems that do not require RDP to be turned on (in Windows 10, right click This PC, properties, Remote tab). RDP is disabled in Windows by default, but if it’s been turned on and it’s never used, it’s a security risk
5) Have a good firewall in the environment, with anti-virus installed to each PC, and servers, too.

If you need help with these prevention techniques, please reach out to Mark Berger or John Woods at Keystone Technologies – we will be happy to facilitate a “Ransomware Preventative Site Visit,” where we will implement the above procedures to safeguard your network. Please call us at 519-451-1793 extension 207.