Custom Computer Specialists
Right People. Right Results.®

Ten Tips for Developing a Ransomware Defense Strategy

Dennis O’Connell
Director of Healthcare Solutions
Custom Computer Specialists

Just when you thought you had a handle on the myriad threats to your network environment, enter Ransomware. Ransomware is a nefarious form of malware that does exactly what its name suggests: holds your data or network hostage by encrypting it with a password. To get your data and/or network restored you must pay a ransom, which is generally required to be made with untraceable funds, like Bitcoin. The ransom varies, and it is a common ploy of the perpetrators to double the ransom if it is not paid within a specified period of time. Once the ransom is paid, you’ll receive the password to unlock your data and network.

The good news is there are ways you can avoid becoming a victim of ransomware. Here are some tips to keep in mind as you develop your Ransomware defense strategy:

1. **Strong backup plan:** It is imperative that you have a solid back up plan to effectively deal with Ransomware. The capacity to retrieve your files may be your sole option. Ensure that your backup process is practical and diversified, and that your data is backed up to an offsite location.

2. **User awareness:** Almost all Ransomware is spread through email attachments. Train your employees to identify emails and to not click on attachments that seem suspicious. Specifically, be on the lookout for attachments with double extensions, such as *filename.pdf.exe*. The .exe may be hidden to trick users into thinking the file is just a harmless pdf.

3. **Use anti-spam software:** When configuring your email server, choose to block the delivery of suspicious attachments, especially ones with attachments with extensions like .exe, .vs., or .scr.

4. **Allow authorized users only:** Restrict access to authorized personnel. Instruct users to employ strong passwords, that they don’t tape to the bottoms of their keyboards. Passwords should be changed regularly to reduce potential risks.

5. **Update your computers:** With thousands of new malware variations appearing daily, ensure all of your software is up to date, including your operating system, browser, and all of the plug-ins that a browser uses.

6. **Have an action plan:** Now, more than ever, you should revisit your business continuity plan to ensure it includes protection from these growing and evolving threats. How do you back up your data? Establish your response beforehand with clear instructions of who to call, how to reach them immediately, and where passwords, install disks and recovery tools are located. The moment you recognize a breach, turn off the Internet connection to the affected device. If Ransomware cannot establish a connection, it cannot complete the encryption process.

7. **Use your firewall:** Because of the essential protective quality of firewalls, they maintain a defensive posture against existing and evolving malware. You are more apt to discourage a potential breach with a strong firewall.

8. **Define software restriction policies:** Prevent executable files from running in specific locations on your computer. Make an exception for software that legitimately needs to run in this area rather than the Program Files area.

9. **Restrict mapped drives:** Ensure that server drives are only mapped to the user where they are actually needed. Use read-only folders where possible. If an infected machine cannot access the server drive, it cannot infect it. Pay particular attention to cloud drives, as they are vulnerable as well.

10. **Multi-layer security protection:** Employ a security solution that addresses protections for file-based threats through traditional anti-virus software, download protection, browser protection, and firewalls. The use of both anti-malware software and a software firewall enables you to recognize threats or questionable behavior.

CONCLUSION: The best offense is a good defense. A strategy that integrates awareness, prevention and recovery with proven security precautions is the best strategy. A fully practiced and repeatable backup and recovery process is the most effective defense against Ransomware.