Best Practices to Protect yourself against Ransomware

Ransomware is a malicious software that cyber-criminals use to hold your files (or computer) for ransom and requiring you to pay a certain amount of money to get them back by encrypting your files. Since its been discovered, Ransomware has been growing at a tremendous speed with more and more users being infected, both companies and consumers. This is critically affecting the productivity & reputation of many companies, which many of them are paying in the end.

Even if your organization is not protected by a comprehensive network security solution like Sangfor NGAF, there are still a few things that you do to prevent or at least minimize the damage.

1. Backup Your Data

Not only against Ransomware, doing a regular backup of your data can help you whenever your computer or network encounter a failure. Remember to do it on an external driver (better if password protected), which should be disconnected when not in use. This will avoid any access from it by Ransomware.

2. Show Hidden-Files extensions

By default, some Windows systems will hide known file-extensions (e.g.: “FILE.PDF.EXE”), so people might not be able to recognized a potential threat when they see it. Cyber-criminals know about this and will disguise the file under another name. By enabling show hidden-file extensions, you will be able to easily spot suspicious files.

3. Make Sure Your Computer is Up-To-Date

Many cyber-criminals will rely on existing vulnerabilities of users running outdated software to get access to their computer. Whenever possible, remember to do regular update of all your software, including OS system, and if possible let it run automatically for better convenience.

4. Do a System Restore Whenever Necessary

Remember to enable System Restore (if you are using Windows) whenever possible. This might help you to take back your system to a state before being infected by Ransomware.

5. Disable Remote Desktop Protocol (RDP)

Cyber-criminals might get access to your Computer through Remote Desktop Protocol (RDP), which is a tool available in Windows to allows others to access your desktop (for technical support & others). If you do not use it in your company, it is a good idea to disable it just in case.

6. Be Quick: Disconnect Your Internet Connection

If you suspect that your Computer got infected after opening a file with Ransomware, disconnect all connections to Internet IMMEDIATELY by closing your Wi-Fi connection and/or unplug your LAN cable. This will delay or stop the communication with the C&C server before it finishes encrypting your files, and if you are lucky, it might save you.

7. Filter “.EXE” files in Emails

If your Company has a gateway email scanner and if it can filter files according to their extension (e.g.: .EXE), it could be a good idea to deny emails with the .EXE extension as it is really not often used on a daily basis.

8. Use a Reputable Anti-virus, Anti-malware and Firewall solutions

Even if this is only useful on a user-basis, it is always nice to have your own computer protected with a good anti-virus, malware and firewall solutions to help you identify and stop potential threats. There are many free software’s available on Internet, so if you do not have one at the moment, go and download them now!

9. Disable macros in Microsoft Office files

Microsoft Office documents containing built-in macros can contain embedded code written in programming language (VBA) and be dangerous as they can become a potential vehicle for malware such as Ransomware. Disable it for further security.

10. Last but not the Least, Educate your Users!

All the above advices are only useful if followed by every employee in the Company. That is why IT managers

have to make sure that everyone knows about the risks of Ransomware, what it could do, and how to protect yourself or at least minimize its damage.

How Sangfor NGAF can help Organizations

Sangfor NGAF is the world 1st fully integrated NGFW (Next Generation Firewall) + WAF (Web Application Firewall). It can help you provide a comprehensive network security protection against current, emerging and future threats.
Below are the main tools integrated in Sangfor NGAF that can help prevent your Organization being affected by Ransomware.

• Anti-Phishing: Send out alerts on suspicious emails that could bring in Ransomware.

• Anti-Virus: Clear out known Ransomware according to over 1+ million signatures in SANGFOR database.

• Sandboxing: Detect and block emerging and new Ransomware by cloud-based threat analysis.

• Anti-Malware: Damage remediation - keep Ransomware from spreading via corporate network and even block the encryption process.