T2021_21 Risks of File Sharing (15th December 2021)

What is File Sharing?

File sharing is the practice of using technology that allows internet users to share files that are on their individual devices. Peer-to-peer (P2P) applications, such as those used to share multimedia files, are some of the most common forms of file-sharing technology. Peer-to-peer applications also introduce security risks that may put your information, your computer or your network in danger.

Risks of file sharing technology

File sharing technology poses great risk to information, devices and networks. Some of these risks are:

- Exposure of sensitive information- when using peer-to-peer applications it is highly likely that you may be giving other users access to personal information. When you make certain directories or information accessible to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it.

- Installation of malicious code- When using peer-to-peer applications, it is difficult to verify that the source of the files is trustworthy. Attackers often use these applications to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When you download the files, your computer becomes infected which can further spread to your entire network and put your organization and its information at risk.

- Susceptibility to attack- Some peer-to-peer applications may ask you to open certain ports on your firewall to transmit the files. However, opening some of these ports poses a serious threat because it may enable attackers to attack your computer by taking advantage of any vulnerabilities that may exist in the peer-to-peer application. There are some peer-to-peer applications that can modify and penetrate firewalls themselves, without your knowledge.

- Denial of service- Downloading large files may cause a serious amount of traffic over the network and due to this a user may see a reduction in the availability of certain programs or services that can be accessed over the network.

How to minimize risks of file sharing

The most effective way to eliminate risks of file sharing is to avoid using peer-to-peer applications but in cases where you choose to use these types of applications you may want to have good security practices to minimize these risks.

- Install and maintain a trusted anti-virus software. Anti-virus software are trusted with the responsibility of recognizing and protecting our devices against viruses but one thing to note is that attackers are continuously working on creating and innovating attack methods, so it is therefore important to always ensure that your anti-virus software is always up to date.

- Install or enable a firewall. Firewalls may be able to prevent some infections by blocking malicious traffic before it can enter your computer. Some operating systems include a firewall, but you may need to make sure it is enabled.

- Educate employees. Most employees do not understand the risks that peer-to-peer file-sharing poses. They may know they're not supposed to use them, but without understanding why, they may decide to ignore the rules and do it anyway. Companies who explain to their employees the reason that file-sharing networks are off-limit increase the chances that those employees will comply with the rules.

- Store sensitive data in a secure location. Data breaches occur when files are easy to access; storing them in a secure location, such as in a secure virtual data room, makes it almost impossible for someone to accidentally share important documents, and makes it much harder for attackers to access that information as well. Secure virtual data rooms have extra protection, multiple levels of authorization and track who accesses files. This makes it easy to monitor them for inappropriate usage and to keep sensitive data safe.

The Guyana National CIRT recommends that users and administrators review these recommendations and implement them where necessary.

References

- Masin, Julie. (16th February 2013). Peer-To-Peer File Sharing Risks. Retrieved from Securedocs: https://www.securedocs.com/blog/2013/02/peer-to-peer-p2p- file-sharing-risks

- McDowell, M., Wrisley, B., & Dormann, W. (17th September 2019). Risks of File- Sharing Technology. Retrieved from CISA: https://www.cisa.gov/uscert/ncas/tips/ST05-007