Ransomware: What to do?

Nowadays, malware attacks, have become very sophisticated and advanced. One of the biggest attack threats today is the ransomware, malicious software that quietly works in the background of your computer or server, in order to encrypt user documents with a secret cryptographic key, making it difficult, and almost impossible, for users to recover unless the ransom is paid.

Several organizations have to pay considerable sums to hackers in order to get back their important files. It is very difficult to overcome ransomware but there are some “to-do” tasks in order to avoid attacks or protect your business before and after an attack.

- Use antimalware software: There is no better way to avoid malware, other than prevention. Antimalware software recognize, remove and prevent ransomware. New definitions are likely to detect and remediate the ransomware.
- Backup your computer and servers regularly: Backup is very important and you need to use it always. A company without a backup is a driver without insurance. Make sure that you back up often. If you back up files to either an external hard drive or to backup service, you minimize the possibilities, even though at some occasions the hackers used the ransomware to delete all the backups.
- Lock down mapped network drives by securing them with a password and access control restrictions: Use read-only access for files on network drives, unless it is absolutely necessary to have write access for these files. Restricting user permissions limits which files the threats can encrypt.

IBSCY Ltd managed to recover most of the files of the clients that attacked from ransomware but prevention is the way to go.

Chrisanthi Christodoulou

Systems Consultant

IBSCY Ltd