BaQapp

The safe backup solution

PRESS RELEASE **For immediate release**

10 May 2016

What are safe backup solutions?

Forget about anti-virus as protection, because new ransomware may not be detected.

It's similar to wearing a seat belt. You have less chance of harm, but you can still suffer damage.

You could try Software Restrictions Policies where the PCs can only run authorised applications, and hope that they will not trigger the ransomware, although you then require competent administration with increased overhead.

The simplest is cloud backup. The main limitations are access speeds, especially in the Australia where our internet speeds are rated 46th in the world, even behind Fiji. This can be a problem for both uploading and recovering large files, and a bigger problem if an image backup is required where an entire drive of only 100 MB can take 24 hours at 10 Mbps, about the average Australian internet speed.

However unless your cloud backups include a versioning option, they might be useless against ransomware attack where a recent infected backup overwrites an older clean backup. Cost is not a relevant factor in cloud storage rates, with prices as low a MB a cent a month, but the costs can mount up for data transfers.
Cloud storage is a privacy concern for some.

Cloud-based data is backed up, but only to protect the cloud provider, not the organisation. If, for example, you or an employee deletes files, there is little that can be done to recover them without paying restore fees. Cloud-to-cloud backup protects against this type of data loss.

Cloud-to-cloud backup provides users with a convenient way to have data stored in many locations. However, it also multiplies the possibility of sensitive information being compromised, in particular as compared to offline hard backups, as well as adding costs.

And although cloud has generally proved to be a more reliable backup method than local efforts tend to be, any system can fail or be compromised, and you can be certain that some geeks are working on how to do it. Multiple locations are advised for backups for added data security.

USB drives

An attached or removable USB drive is cheap and simple. However a connected or mapped drive will be infected only fractions of a second after your main data, making the backup useless. Many technical writers wrongly suggest only connecting your USB drive while actually making the backup is OK. IT IS NOT. First of all human nature as it is, means that it will not be connected often enough to ensure current backup availability. Then having been connected, after making the backup it will be remain connected and will become infected.

Anyway in the long term, disconnecting your USB backup drive won't help against sophisticated malware that specifically looks to encrypt/destroy your backup drive connected for even a brief moment, and only then encrypts your main drive...

NAS Backup Appliance

The real solution is to use intelligent/network backup systems (NAS backup Appliances) that have "Read" permission of your data, but your PC doesn't have "Write" permission on their storage device... In other words, don't trust USB backup systems - use only IP based solutions (including network shares/NAS).

The high end units will protect large amounts of data and have high speed interfaces, but can cost from thousands of dollars to tens of thousands of dollars since they are designed for larger organisations.

The low end units are usually designed as servers. Many will offer unsophisticated USB backup solutions which are useless to prevent ransomware infection of your backup device with viruses/rootkits, unless someone configures/secures it properly which does take some technical know-how.

BaQapp

The BaQapp Backup and Recovery Appliance is a low cost solution with all the essential features of the high end backup appliances without the complication and cost, Mainly to protect against ransomware BaQapp hardens (seals, or vaults) the backup storage against malware attack, and automatically makes regular versions of the backups.

The BaQapp backup appliance provides a fast, easy-to-use, and affordable data protection for businesses. The backup appliance is a complete backup solution for Windows, Macintosh and Servers that delivers a network backup server and client software, integrated OS, optional RAID for disk backup, and optional replication. It is ideal for offices without full-time IT resources, or for those that just wish to simplify deployment and management.

The BaQappBoxx appliance is available on our ready to run ARM hardware,

The BaQappVM appliance will also run as a Virtual Machine downloadable with 30 days free trial, where there is an existing virtual environment using VMware vSphere, Microsoft Hyper-V, VirtualBox and selected QNAP models.

The BaQapp-x64 appliance is for use your own, compatible "bare metal" x64 hardware which does require a bit of Linux know-how to install, or can be installed by a BaQapp reseller.

- BaQapp backup appliance has a web-user interface
- Unlimited numbers of file/folder/disk image backup agents
- Deduplication
- Network data segregation, making backups resistant to Ransomware

The real solution is to use intelligent/network backup systems that have "Read" permission of your data, but your PC doesn't have "Write" permission on their storage device... In other words, don't trust USB backup systems - use only IP based solutions (incl network shares/NAS).

USB backup solutions are bad for infecting your backup device with viruses/rootkits anyway... With a NAS, if it writes/copies infected exe's (or any file) to its hard drive, the actual backup device won't get infected (thus spreading the malware to other files on it) until someone executes these malware - which will never happen if you configure/secure it properly...