ABTECH TECHNOLOGIES

StorTrust

RANSOMWARE!

How a Good Backup and DR Solution Can Protect Against It

By Nigel Wright, VP Sales, Enterprise Solutions, Abtech Technologies

WHAT IS RANSOMWARE?

Basically, ransomware is a malicious tool that encrypts all the data on the infected system. It is often emailed to unsuspecting staff as an attachment to an official-looking email. They open the attachment and their system is encrypted. If not spotted immediately this can spread to other systems they are connected to.

Shortly after, the recipient receives a ransom demand. You have a certain amount of time to pay the ransom, or all your files will be deleted. Once your computers are infected, it can be very difficult to remove. In fact, some law enforcement agencies have even told victims that the only way out is to pay the ransom.

Overview

In a modern business, access to IT systems and the data that resides on them is critical to the functioning of the business. It you can't access this data your business will grind to a halt and you may be faced with long delays while the problem is fixed. Try turning of email and wait a few minutes for the CEO to be on the phone to the IT Department demanding answers. If you can't access your file server or email server, your staff can't do their job.

This increasing reliance on data has led to the increase in ransomware attacks against businesses of all sizes. Businesses that rely heavily on their data will pay large sums of money to get it back, rather than risk the loss off revenue and image. The modern cybercriminal knows this and will exploit it whenever he or she gets the opportunity. It is the new blackmail and the level of sophistication being used by hackers to infiltrate businesses with ransomware is increasing.

IT Web suggests that the total cost of data security breaches will be more than $2.1 trillion by 2019. The majority of these affecting small and medium sized businesses will be some form of ransomware.

Will Traditional Backup Protect You?

"We have backups" you may say. But do you have the right backup solution that will protect you and do you have a disaster recovery solution?

- **Do you have a backup solution that allows you to roll back to just before the infection arrived and restore a clean system?**
- **Do you have a BDR solution? This is where the backup solution is tightly integrated with a disaster recovery solution, usually in the cloud, where you can spin up your critical systems at another location.**

You will be able to recover from a traditional tape backup, but that takes time and you may lose an entire day's worth of data. There is always the risk that the restore doesn't work, so you have to go back to earlier backups, if you have them.

How does a Backup and Disaster Recovery (BDR) Service Help?

Let me give you an example:

One of our managed services customers recently experienced a ransomware attack. A member of staff was sent an email with a Crypto locker virus attached to it. This is a widely used piece of ransomware, which encrypts the files on the computer it infects and any directories on other systems it has access to.

The email looked genuine and was addressed personally to that staff member by name, so he opened it.

Immediately his system was encrypted. The virus also encrypted the company file server so none of the users could access their data. Everything ground to a halt.

Shortly after a ransom request arrived in the user's inbox asking for a sizeable amount to be paid in bitcoins.

The CEO and CFO were alerted and, after a short period of mild panic and discussion, they called Abtech for advice.

Fortunately, they were signed up to our StorTrust Backup and Disaster Recovery (BDR) services. The service uses Quest Rapid Recovery software that is configured to take snapshots of their systems every 30 minutes (it can take Snapshots every 5 minutes, but this customer preferred every 30). The data is then replicated to our StorTrust cloud data center in Nevada, for disaster recovery purposes.

The StorTrust engineer checked the logs and found that the last good backup happened 5 minutes before the ransomware attack. This meant that we would be able to recover the data to a clean file server and the client would only lose 5 minutes' worth of data.

The client agreed and we restored their infected server from a clean backup. The user's system was also reimaged and data restored from the backup. The whole process took less than an hour and no ransom was paid.

If the infection had been more widespread, we would have elected to spin up their critical systems in our cloud, using the replicated good backup, so their users could continue working, while we cleaned and restored all their infected systems.

Key Takeaways:

- ✓ **No ransom was paid**
- ✓ **Only 5 minutes of data was lost**
- ✓ **Total downtime was less than 1 hour.**

Without the StorTrust BDR solution in place

- ✗ **Ransom of several thousand dollars would have been paid.**
- ✗ **This would have taken some time whilst the CFO worked out how to pay in bitcoins.**
- ✗ **The client would still be seen as a good future target for the hacker because they had to pay the ransom.**

ADDITIONAL BENEFITS OF A BDR SOLUTION LIKE STORTRUST

1. **Protects the business against disasters. Whether it's a natural disaster, a power outage or the more common, human error, it will protect your data and ensure that downtime is minimal.**
2. **Deleted files can be recovered quickly. No searching for tapes or waiting for tapes to be retrieved from offsite storage.**
3. **A single interface so no need to have staff dedicated to maintaining the disaster recovery solution. In the case of StorTrust, it just requires a phone call.**
4. **Compliance. Your customers may have rules about protecting any data they share with you. If you are an important supplier, you may need to guarantee uptime. A BDR solution will provide this.**

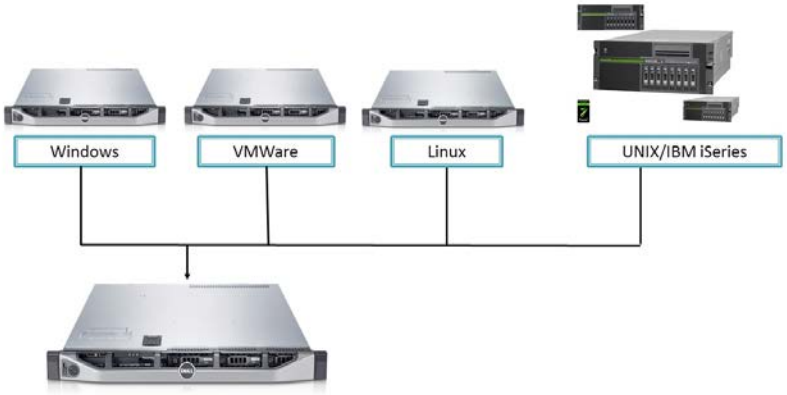
What is StorTrust?

StorTrust integrates Backup and Disaster Recovery into a single solution. It is available as a local backup and recovery solution or a complete backup and cloud disaster recovery service.

StorTrust Local Backup and Recovery

At the local level, backups are managed by a local appliance running Quest (formerly Dell Software) Rapid Recovery Software or Veeam.

The backup software can be set to take regular incremental backups, which is important to rapid recovery of clean data. As we found with the example earlier, having a recent clean backup is vital to recovering from a ransomware attack with minimal data loss.



StorTrust Cloud Disaster Recovery

StorTrust provides additional protection as a cloud disaster recovery service. The backup software on the appliance deduplicates and compresses the data before replicating it to our secure StorTrust datacenters. This provides both an offsite backup and a disaster recovery solution.

We are able to spin up a damaged or infected system in the StorTrust cloud servers. The recovered system is built from a clean, uninfected backup in the same way as it would be locally.

This is unique in that it is a managed service. There is no need to access a dashboard or Web interface to spin up the servers in the cloud. If our customer experiences a disaster of any kind, they just need to call us up and we will do the rest.

Complete Protection against Ransomware Attacks and Disasters

For further information or to arrange a demonstration, please contact us:

1-800-474-7931

info@abtechtechnologies.com

www.abtechtechnologies.com

ABTECH TECHNOLOGIES