For Immediate Release
Monday, March 4, 2019

# Does Your Disaster Recovery Plan Work?

It is often said that a Disaster Recovery Plan is only as good as it works in practice. This concept was put to the test for a client recently after their Hyper-V host was hit with a full disk encryption attack caused by a ransomware virus that renders the entire system useless. Of course, the first thing anyone in this situation asks is, “How could this happen?” But the real question is, “Can we recover?” The answer is not always, YES.

Luckily for this client we had them on our Hybrid Cloud based backup service for several years. This service creates a fully encrypted backup in the cloud keeping it safe from this type of attack. As a part of the service, we periodically restore protected systems to a dedicated server in our shop, then test these restorations to make sure it is working properly. When the client asked, “Can we recover?” We were confident we had it covered.

We received the call from the client early on a Friday morning. Upon investigation, they were hit with a “Mamba” ransomware. This is a particularly devastating attack because it not only encrypts files, it also encrypts the Master Boot Record on the hard drives rendering them completely inaccessible. The server was unrecoverable. We quickly decided that the best course of action would be to kick off a full restore of the clients VM to the recovery server in our office. Meanwhile, we pick up the client’s server, brought it back to our shop to start the physical rebuild of the Hyper-V Host.

During the recovery process, we were in contact with companies that claimed they could recover the system from the attack. The problem with these services is they are provided at a premium cost with no guaranty of success. Upon request from the client, it was decided to completely replace the eight drives in the Hyper-V host and hold the affected drives in case they wanted to send them out for recovery. We informed the client that this would delay restoration, but they were insistent that the drives be replaced and the original drives kept in case we weren’t able to fully recover. We placed an order for eight 2TB server class drives, and the rebuild was put on hold until the drives were received.

Meanwhile, the restoration of 3TB of data was proceeding on our restore server. The question here was how long would a full restore take? Our shop does have a 1gb internet connection, but the progress indicated fluctuated between days and hours.

With Friday behind us, Saturday started with the restoration done! 3TB of data restored in roughly 24hrs. With a couple of clicks in the Hyper-V Management console the restored VM fired up and ran perfectly. After a cursory look over the data drive, we had all the data intact and ready to go when the Client’s host was ready.

The new drives arrived on Monday. We immediately installed them and started the RAID configuration, only to find one of the eight drives was bad. Dead without all the drives, we overnight a replacement and put the project to bed for the night except for running full virus/malware scans on the restored VM and data just to make sure we weren’t reintroducing an infected system. These scans came back clean.

The replacement drive arrived Tuesday and was added to the system; RAID created and Windows 2012r2 installed. After which we installed and configured Hyper-V. Once Hyper-V was up and running, we created a new machine for the restored system and began a copy of the VHDx files from our restore server.

With the client's VM now up and running on its proper host server we turned to restoring a MySQL server database contained on that server. MySQL restore started, a full 790GB of additional data to restore which took a few hours to complete. By the end of the day on Tuesday we had the client's server backup and fully functioning.

In conjunction with the MySQL restore, we recreated a Remote Desktop VM that the client users use to connect to the system and do their daily work. You may ask, "Why wasn't this included in the backup plan?" The answer is simple; the client didn't want to pay for additional cost of backing up a VM that never changes and can be rebuilt quickly. Once we had the RD up and running, we redirected the users to access it while the server at our shop and asked them to give it a good work over and verify everything was restored and running properly. The response from the client was, of course, great relief as all their data was there and the system was running normally.

Lessons to Learn:

1) Had the client NOT employed our Hybrid Cloud Backup services, they could have been completely lost their data and potentially their business. This kind of attack not only targets internal storage, but it also hits externally connected drives that are commonly used for data backup in the SMB world. Had the client's backup been stored only on one of these USB connected drives, the backups would have also been destroyed.
2) Testing your backup plan is crucial. Had we not periodically tested the data being backed up there would have been no way we could have provided the client reassurance that their data was recoverable.
3) Had the client not made the request for new drives we could have had them back up and running within one business day. Time to restore is as critical as being able to restore in the first place. The drive swap cost the client two business days. Nevertheless, we had their systems fully functional with in 24 hours of the attack and back on line for use within 3 business days.

In conclusion, it is no longer enough to simply backup your systems to on site storage locations such as USB drives, NAS storage or other systems. Most attacks seek out these systems and destroy them too bettering the attacker's chance of receiving tens of thousands of dollars in ransom payments with no guarantee of recovering your data. The only way to completely protect your systems is by using a properly designed and tested off site Disaster Recovery Plan.

RRK Associates officers a full suite of cloud based and hybrid cloud backup services to help prevent total loss of data. Backups are encrypted (military grade encryption available) at the source and stored in redundant storage facilities in the US. As a part of that service, we continually restore and test your backups to ensure they are working properly. Remember your Disaster Recovery Plan is only as good as it works in practice.

For a free assessment of your current Disaster Recovery Plan please contact us at (202) 237-8703.