ISSN:2249-5789
Muppalla Prudhvi , International Journal of Computer Science & Communication Networks,Vol 3(2), 97-100

DISATER RECOVERY ON DOUBLE DUTY USING CLOUD

Muppalla Prudhvi
KL University,India.
Prudhvi.muppalla@gmail.com

Abstract

This paper describes how the virtualization and replication technologies will protect the data from the disaster without any loss to the business. From past 2 years the IT department has been reducing the costs and they are meeting there services and the commitments of disaster recovery are made successful by using the hybrid cloud which is made up of two virtualized hardware. Since paying more to the dedicated recovery hardware most of IT companies use virtualization hardware which reduces the risks and workloads. In order to make disaster recovery as another service more and more IT shops are using the virtualization and replication technologies.

1. Introduction

Most of the IT shops are using the virtualization and replication techniques which makes the disaster recovery just as a service, sometimes they can use same servers and networks and storage which runs the order entity or email application development and any other services. This says that how the disaster recovery and other business continuity efforts which helps to protect the business not only from the disasters but also from the human error or from the equipment failure. Some stores only data which allows the physical hardware to run them when there is a need of it. There are more demands as well as more risks. In order to make all these changes and make everything upto date they are reducing their costs and the flexibility provided by the server, storage and also the virtualization networks. In the report of forrester it is mentioned that the enterprise disaster recovery and business is get stuck and most of the priority for spending are done on consolidation, business intelligence and virtualization.

2. An Overview of Virtualization

Virtualization was used mainly in testing and development for IT departments of all sizes over the past few decades and now its playing a pivotal role in production environment too.

The concept of virtualization can be explained in a simple manner— first you run a piece of software application on a PC . In the software (virtual machine), you can install the operating system (OS) of your choice and install any applications you need. Hence, on one PC many virtual PCs are created, each of them running an OS and software applications of its own, independent of the OS and the applications you are running on the main (host)PC.
What stands between the hardware and the guest OS is defined as a *hypervisor*. In computing, a **hypervisor** or **virtual machine monitor** (**VMM**) is a piece of computer software, firmware or hardware that creates and runs virtual machines. Typically on standalone systems, the hypervisor runs off the conventional OS that you might be using, whereas a hypervisor that runs directly on the bare metal or as close to it as possible is amore server-oriented virtual machine(VM) architecture that you would look to when considering virtualization and data protection.

3. Best Method for Disaster Management

The best method is that we can have the cloud based data recovery service. By separating the networks, virtual servers and storage capacity from physical hardware and virtualization gives many more choices for the disaster recovery. Disaster recovery can also be done very fast and it is very easy to replicate the software which copies the data between the primary and recovery sites in the real world. VMware integration improved all the backup and recovery tools by making it easy to replicate and restore not only the servers but also their databases and security systems. In order to restore a business services in a successful manner the IT must recover the application server and also the associated components in an order. So we have to focus mainly for vendors by taking all these into consideration.

In order to have a good business the major goal for a vendor is to have a fast recovery. If we improve the performance of the replication system and also the related technologies such as a snapshot tools and

making them to have a shorter virtualized disaster recovery is the main goal for the vendors. Most of the PAS applications allows the user to the data for time and then it will transfer the data for the remote page and the changes in the data only will be send to it. So by this application we can eliminate the backup need but it doesn't reduces the bandwidth. So if we use distributed file system object in the PAS application which has separate blocks for each and every data. So that we can reuse the data for the disaster recovery purpose.

Because of using all these virtualization functionalities the disaster recovery systems can make a pay. The only one way in which the disaster recovery systems can get more funding is they have to demonstrate that they can deliver more and they have show that they can pay for themselves. To take the snapshots every hour the bandwidth is also so helpful. Thus snapshot helps to justify the cost of the disaster recovery without any disaster. Another benefit is the virtualization allows the IT companies to use dell compel lent storage which is paid more on the platform of the recovery for its newer version called XIO tech storage. Most of the providers says that this cloud based disaster recovery will really gets benefits for the true disaster recovery when compared to the backup to small and medium size businesses. The provider for the public cloud data says that most of the customer are totally satisfied and there is an increase in the customers who are satisfied with this cloud security. Most of the security experts says that even in the public cloud environments a hardware can be shared by multiple customer which can also be made secure if there are proper processes.

4. Types of Disasters or Security Test

Fig.1.types of disasters

4.1. Natural Disaster

No one can stop the natural disasters like fire, lightning, floods, hurricanes and earthquakes which can cause fierce damage to the computer systems. So at that time information can be lost, loss of productivity can occur and hardware damage may effect the essential services. There are some safty methods which can be implemented against these type of disasters.

- The best method is to have contingency plans and recvovery plans in place.

4.2. Human Threats

The most dangerous among the human threats are former insiders, because they were aware of many codes and security measures which were implemented. They will access to the systems through which they can access many applications which are used and they were aware that which actions will cause the most damage. They may plant worms, horses and trojan and they can access the file system.

One more type of human threat was Malicious attackers. They will have a special motive, objective or goal for their attack on a system. Hackers can sell information that can be useful to competitors. They might also want to steal information or even steal hardware such as laptop computers. Thier main motive is to to disrupt services and the continuity of business operations by using denial-of-service (DoS) attack tools.

The different threats and their motives were sown in the below figure.

Threats	Motives/Goals	Methods
• Employees • Malicious • Ignorant • Non-employees • Outside attackers • Natural disasters • Floods • Earthquakes • Hurricanes • Riots and wars	• Deny services • Steal information • Alter information • Damage information • Delete information • Make a joke • Show off	• Social engineering • Viruses, Trojan horses, worms • Packet replay • Packet modification • IP spoofing • Mail bombing • Various hacking tools • Password cracking

Fig.2.types of threats,motives and their methods

Figure that gives a theoretical model that can be used to determine the various threats, goals, methods, and vulnerabilities used in an attack:

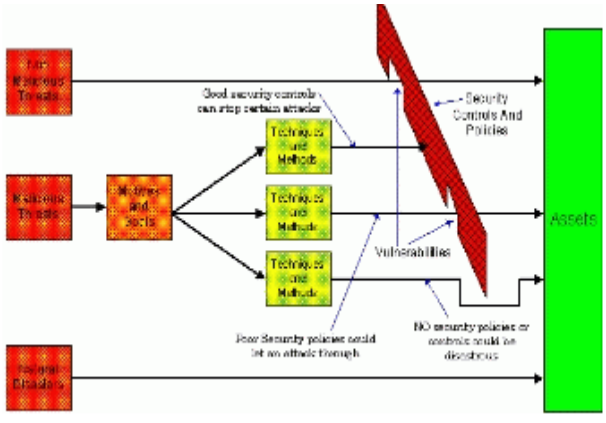

Fig.3.model to determine threats,goals and methods

5. Real Time Examples

1. One of the employ use to bring games and made them to run in his local system. Unfortunately the employs of the company seen sudden changes in their systems due to the fires in the games which was accessed by one of the employee. This comes under non-malicious threat (ignorant employees). The following figure explains the various vulnerabilities that existed and the loss in assets that are involved.

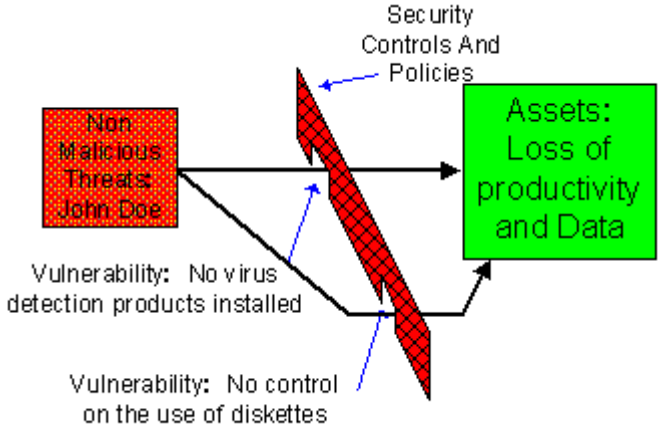

Fig4.employee attack.

2. One employee was fired from the E-commerce company due to some reasons and he thought of taking revenge against his manager. He made the company's web server to accept requests by using a denial-of-service attack tool called Trin00 to start an attack on the company's Web server. The customers started complaining that they cannot connect to the web server. malicious threat (malicious attackers).The following diagram outlines the various tools and vulnerabilities Sally used to achieve his goal.

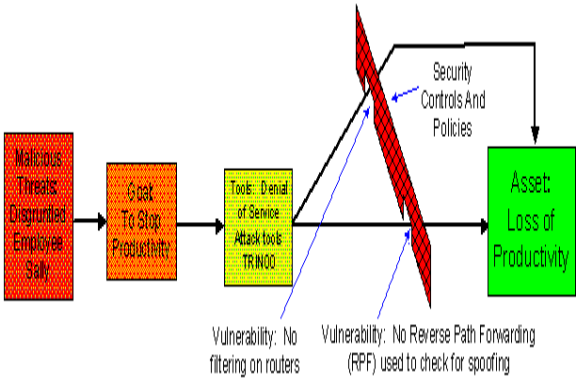

Fig5.miscallenous attack

3. In a company during a thunderstorm, lightning strikes the telephone and ISDN lines. All modems and ISDN routers are destroyed, taking with them a couple of motherboards because of not having the surge protection. This comes under Natural disasters. The following diagram shows the vulnerability and the loss of assets.

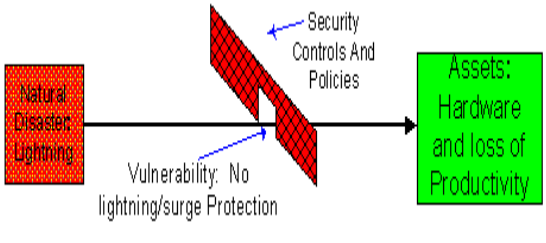

Fig 6.natural disaster

6. Conclusion

I do agree with this because both the virtualization and replication technologies protect data from the disaster. They have so many options and most of the IT technologies are using the same virtualization and recovery hardware to reduce the disaster. There are more demands for this cloud recovery and also more risks. The recovery in cloud can be done by using the data recovery services. And also most of the customers are liking and satisfying with this technology. And also the use of snapshot tool improves the performance and replication. There are some new approaches to the data recovery and they are using portions for the backup of sites to store the images for the sites. And many organizations are reducing or ending their use of tape for disaster recovery, although some still use it for long term archiving. Most of it shops are expanding disaster recovery to include not only servers, but also user devices. They are using portions of backup sites to store all the images of virtual desktops, laptops or even tablets so users can have access to their data and applications while they await replacement devices. Many companies optimize the performance of the network to speed backup and replication from branch offices to central data centers. And many of the organizations are reducing or ending their use of tape for disaster recovery, although some still use it for long term achievement. Most of the smaller companies do choose the cloud typically don't do it for savings. Most large organizations are big enough to provide disaster recovery by themselves. Most of the cloud disaster recovery is also not suited for most of the applications in this present situation and they rely on the older platforms which does not provide the cloud, and large databases also do not perform the cloud.

7. References

[1]Peter Gregory and Philip Jan Rothstein,"IT Disaster Recovery Planning For Dummies",Wiley Publishing, Inc.,Dec.2007.

[2]Regis J. Bates,"Disaster recovery planning: networks, telecommunications, and data communications",McGraw-Hill,1992.

[3]Brenda Phillips,"Disaster Recovery",CRC Press,Mar.2011.

[4]Michael Wallace and Lawrence Webber,"The Disaster Recovery Handbook: A Step-by-step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets, Volume 2",AMACOM Div American Mgmt Assn,2004.

[5]Charlotte Hiatt,"A Primer for Disaster Recovery Planning in an It Environment",Idea Group Inc (IGI),2000.

[6]Zhang Jian-hua ,"Cloud Computing-based Data Storage and Disaster Recovery" at Future Computer Science and Education (ICFCSE), 2011 International Conference

[7]J Peter Bruzzese,"Virtualization And Disaster Recovery",Realtime Publishers,2009