Cloud Computing & Data Backup

Submitted to: Dr.Kevin E.King

Cybersecurity 6

01/15/2021

Mokshita Mannam

Cloud Computing & Data Backup

Introduction:

Cloud computing is a new technological advancement that has users growing by the day. Cloud computing has two definitions. The first and most common is called a public cloud model. It runs data remotely over the internet in a commercial provider's data center. One popular public cloud is Amazon Web Services. Most businesses though take a multi cloud approach, which means that they use more than one public cloud service (Knorr, 2018). The second meaning of cloud computing is describing how this system works. It is a virtual pool of resources that are available on demand. When the cloud service is obtained by the customer, the provider fills the requests using modern automation. The main advantage of this is that you can compute, store, and network data as well as tap into a large quantity of already built services (Knorr, 2018).

Some customers opt to cloud management platforms to reduce costs and management. This lets you have multiple clouds as if they were one cloud. The only problem is that these platforms tend to limit the customers data storage. Cloud computing can be detailed and risky at times, but is a modern system everyone is using for a more, secure online data storage (Knorr, 2018).

Cloud computing transports data from softwares and databases to data centers. This new piece of technology has several security challenges. Untrusted servers can be the ones behind data loss because of their irresponsibility in handling their client’s data. One big concern for their loss of data could be data integrity verification at untrusted servers. For example, the data storage provider could decide to hide data errors from clients for their own benefit. This could cause the client to lose a lot of valuable information at the fault of the provider (Wang, 2020). Data that is rarely needed for the client could also be neglected by the provider which could cause the same situation to occur or the provider can delete the files. To solve this problem, many plans and models have been made (Wang, 2020). All plans fall into the two categories of private and public verifiability. Even though private verifiability has a higher efficiency rate, public verifiability can allow anyone using the server to challenge for correctness on demand (Wang, 2020).

Access to a recoverable environment means to have a minimal cost and maximum speed, but not all organizations could set up the habitat or stomach the maintenance cost of a recovery site. Therefore, companies tend to lean towards cloud-based disaster recovery solutions as a more efficient way (McCollum, 2016). Also, since not all applications and data are created equal when it comes to recovery measures it is better to have a balance between cost and flexibility. For higher value applications, an asynchronous server replication secures the cloud infrastructure. The replication server acts as the live environment until the original surroundings are restored (McCollum, 2016).

Unexpected events can bring daily operation to a stop and for services to be always available to clients, the organization must recover as quickly as possible. Not having a disaster recovery plan could put an organization at risk of high financial costs, loss of reputation, and a great risk for clients or customers (Gray Leaf, 2020). Cloud-based disaster recovery is getting a lot of attention from IT companies as an alternative. A critical part of the recovery plan is the emergency communications process. There must be a system in place for information to be sent around to your teams, customers, and some to the government. Data back-up and recovery also should be an integral part of the disaster recovery plan (Gray Leaf, 2020). This strategy starts by identifying the data that should be backed up, inserting procedures, scheduling these back-ups, and making sure that the data was backed up securely. Outsourcing may not eliminate the problems, but it can provide a redundant IT environment and plenty of recovery options that the organization might not have (Gray Leaf, 2020).

Every effective recovery plan should reflect on its RTO (recovery time objective) and RPO (recovery point objective). RTO is the maximum time an application or group of data should be recovered within. RPO is the maximum period of time that can pass when an application is lost. Knowing these points will help determine a recovery strategy and solution (Joosery, 2020). There are many reasons that a disaster can occur such as planned outages, failure of network or power, hacker activity, and weather related events. To reduce data loss, there will need to be multiple copies of data in multiple places. Adding different layers adds complexity, which is hard to manage, so copies are easier to replace. Outages can be costly, and businesses can sometimes be hit by financial problems (Joosery, 2020). One common misconception is the difficulty of reaching high availability. There are so many threats ranging from software bugs to server failures and hacked systems. Risks need to be analyzed with the help of the framework and assess the action that will be taken (Joosery, 2020). If the company does not have a recovery plan, the best case scenario with the limited tools is that the server will crash and there will be a sudden power outage (Soni, 2020). The data recovery plan is a great strategy for strengthening the production operations.

The disaster recovery plan (DRP) cannot be set and forgotten; therefore, it must be tested. Many want to change from traditional methods to modern ones because of the growth in complexity (Doherty, 2020). The only important point of testing the DRP is to find hidden flaws in the system, so the situation does not worsen. Also, being prepared for different situations is key. You will have to have all the components at hand to solve the disaster. This will vary between different organizations or businesses. Testing the only way to evaluate and improve your plan to cover any gaps or holes (Doherty, 2020). The DRP is very flexible because it lets the company work on its own plan to better the environment. Therefore, having a DRP and testing it before use is important for a company to thrive. As many are afraid of the exponential increase of change the cloud has brought them, there has been a rise in the number of misconceptions as well.

Literature Review:

Introducing cloud computing is necessary, but talking about the several misconceptions that are confusing many is important as well. While many believe that there is only one type of cloud model, there are actually three available ones for the average user. The first type is the public cloud model which connects and transfers data from the servers to a provider's data center. Some benefits of cloud computing include reducing the time taken to market applications, machine learning and IoT connectivity (Knoxx, 2018). This is called "infrastructure as a service", where they use API (application programming interfaces) to communicate with each other. These infrastructures are used as a service for the public cloud. Software as a Service, or SaaS for short, are used for commercial applications that users interact with on the internet with minimal code (Doherty, 2020). The benefits of a public cloud are that there is scalability, that lets you only pay for what is necessary, lets you view your data and it eliminates the money a corporation must spend in order to make money (e.Week, 2010). Having a public cloud is also better for updates, cheaper, and is faster to upload (Supply & Demand Chain Executive, 2012).

A private cloud model is where technology runs the software, and that data goes to the customer's data center (Knox, 2018). One of the disadvantages for the private cloud is that it has no financial scalability, resulting in paying for more than what is needed (e.Week, 2010). Though the private cloud is expensive, it can be used in the right way, as long as the structure and maintenance are nurtured (Supply & Demand Chain Executive, 2012). A hybrid cloud model uses both software to run your cloud and the data shuffles between your provider's data center and the customer's data center (Knox, 2018).

Currently, the private and public cloud don't have the ability to seamlessly communicate with each other. Though businesses are trying to make this happen, the completely smooth online experience between these two cloud models won't be happening any time soon. For now, you can set standards for configurations, create data models, and try to automatically sync everything throughout both of the clouds. This will allow you to use the cloud well for the modern day (Doherty, 2020). If switching to cloud computing is too complicated, you should seek out a migration plan to help ease you into using cloud computing (e.Week, 2010).

Many believe that the security in the public cloud is completely secure, which can be proven to be false in certain situations. Actually, there is no way for you to know that your data is secure in the public cloud. Your cloud providers automatically store your data in the cloud, from a premade service (Knox, 2018). The cloud allows you to have all of your data in one place. Your personal information, like your finances for example, can be monitored in the cloud. Also, anyone can find your personal data, however, it can be recovered if the cloud provider agrees to assist. There are no compliance laws encompassing data protection and security once it is backed up for your DR plan (Singh, 2017). Even if you request for your data to be taken down, it won’t be gone on all of the databases. Authenticating information received before verification will keep your original data files in check. Private servers are better for storing your data because local servers can be hacked by anyone. This is why people use a TPA. A TPA (third party auditor) ensures that your data is being stored in the cloud.

Having a TPA can help you if your service providers ever lie about an issue, such as Byzantine failures. These failures happen when your computer fails and sends you false information that assures you that there was no problem. Servers can send you incorrect, corrupted, or manipulated data without you personally knowing, but your TPA can stop this from happening and easily locate them. The user can change the TPA to adjust to their needs, by using combinations of data from the original sources to other devices to pass verification checks (Wang, Q., Wang, C., Li, J., Ren, K., & Lou, W., 2020).

Like with having a TPA to stop risks, we need to minimize the risks that could occur as well. You should not be reliant on a single cloud service and use certain ones for the services that they are known best for. This way, you can spread out your data.

Edge computing is a way to distribute your data over several networks, so you do not have to be reliant on only one. This method distributes local cloud data onto nearby devices. This is similar to cloud computing, but they are not the same (Knox, 2018). Though keeping data in multiple places is useful when recovering your lost data, every additional layer of security adds more complexity. This complexity can be hard to manage and it will be more expensive. You need just enough to minimize the downtime for servers. Downtime is when the server is offline and previous data kept will not be backed up (Joosery, 2020). Cloud computers will try to protect the data even though consumer information has been shared in the past. They have intrusion detection, multiple login systems, and encryption. They minimize the risk of cloud computing information from being insecure by adding a multitude of layers of protection with powerful passwords, accessibility controls, and develop applications with regards to security (Graves, 2017).

Data protection uses software for the time right before a virus or a hardware failure. The offline server that you would use during a disaster will be online until the corrupted servers are restored (McCollum, 2016). Cloud providers are the ones that control your data's protections. It is their job to ensure that your data is safe during downtime of a server, and if they did not do that then they would be fired (Singh, 2017).

Cloud computing is safer in private servers than local ones because in private servers it is their job to keep all of the data safe rather than making it into a business (Gates, 2012). They are also more secure because they have more failsafe systems in place and security like firewalls, among other things to ensure that the data they store on the cloud is safe.

Cloud security and the compliance with your data that you share does not create any new issues versus local servers. They have the same security protocols, if not more than you would with a local server (Communications Today, 2014). In fact, many large businesses that value security, like in the government, medical and financial fields use cloud computing. Software updates are constantly needed in cloud computing for better security. Another benefit in the cloud is that all of your data or information is in one place and is easily transportable after the process of setting up. This helps with your disaster recovery plan, and business owners can manage security to the very specifics (Graves, 2017).

The cloud might not erase your problems in the present, but it will definitely help you reduce the amount of work in the future. You will need to move everything to where it should go, then you need to find the correct service for what kind of security you would like to have, because after you run a service, there could be several unconsidered side effects, whether that impacts your security or your files (Scheier, 2009). However, the cloud also provides less IT work, so when the process of setup is complete, you do not have to worry about the configuration. Once that process is complete, your plans should be smooth and you will not need any real people to interact with your data, meaning that your data is secure (Communications Today, 2014).

For privacy and security, a virtual data center works better than a physical one. Normally, information from different servers are constantly being communicated. Someone cannot walk into the databases and steal information easily, such as in traditional data centers where there are guards, cameras, alarms and other strict procedures, using virtual servers has similar methods. With some services, you are allowed to establish your own IP address, control networks, use firewalls and wipe your data from servers after you permanently delete it (eWeek, 2010). After the servers are installed in the data center, the physical factors can be erased, thus resulting in extra space for other components. Almost all hardware and software problems happen in the virtual aspect of servers, rather than with the physical component (Gates, 2012). Overall, the misconceptions about the cloud should be brought up because it is important to understand and resolve. Lastly, although there has been some awareness being spread for the cloud, misconceptions have arised due to the fear of drastic change in the technology environment.

Analysis:

The cloud is a large computer system resource that stores your data, but the cloud recovery process is still unknown to some users. The cloud can be broken into several different areas such as data protection, data recovery, cloud models, and cloud computing. Clearing any misconceptions about the cloud can result in a great technological advancement and help the business industry. These misconceptions have put a pause to let businesses advance into modern procedures and this could become a problem in the future.

In the process of learning about cloud computing, it was realized that there were so many related ideas in your life. For instance, your gmail account is another example of cloud computing. All the data stored here is in the cloud and some other examples are our banking, food delivery, and social systems. Most of them operate by the cloud and this is where our information or data goes. This shows that the cloud is embedded into everyone's lives. The cloud has a huge part in making everyone's lives easier and more efficient.

A world where all of the misconceptions of the cloud are cleared could mean a strive for modern technology. The main reason many are hesitating is because of their fear of change. This fear causes them to oppose this new technological idea and make assumptions. These assumptions are making others to not choose the cloud, therefore, making their own lives harder. Although the cloud has its pros and cons, if we all come to a basic understanding it will have a great influence for the lives of the future generations.

References

Knorr, E. (2018, October 2). What is cloud computing? Everything you need to know now. *InfoWorld.com*. https://www.infoworld.com/article/2683784/what-is-cloud-computing.html

Wang, Q., Wang, C., Li, J., Ren, K., & Lou, W. (2020, October). Enabling Public Verifiability and Data Dynamics For Storage Security in Cloud Computing. Retrieved November 09, 2020, from https://www.researchgate.net/publication/220294018_Enabling_Public_Auditability_and_Data_Dynamics_for_Storage_Security_in_Cloud_Computing

McCollum, M. (2016, September-October). Disaster recovery for data centers: cloud-based recovery gets organizations back to business faster. Mission Critical, 9(5), 22.

Consultants, G. (n.d.). Disaster Recovery. Retrieved November 11, 2020, from https://www.gograyleaf.com/disaster-recovery

Joosery, V. (2020, October). Disaster Recovery for Open Source Databases. Database and Network Journal, 50(5), 5.

Linthicum, D. (2020, June 9). 3 myths of disaster recovery and cloud computing. https://www.infoworld.com/article/3561474/3-myths-of-disaster-recovery-and-cloud-computing.html.

Doherty, S. (2020, August). Why Is It so Important to Test Your Disaster Recovery Plan? Database and Network Journal, 50(4), 3.

Singh, A. (2017, May 11). Top 5 Cloud Computing myths debunked. https://www.pcquest.com/top-5-cloud-computing-myths-debunked/.

Scheier, R. L. (2009, June 22). Busting the nine myths of cloud computing. https://www.infoworld.com/article/2632461/cloud-computing-busting-the-nine-myths-of-cloud-computing.html

Amazon Debunks Top 5 Myths of Cloud Computing 273198. (2010, April 19).eWeek.

Gates, N. (2012, May). 10 myths about cloud computing in Alaska. Alaska Business Monthly, 28(5), 56+.

Soni, V. D. (2020, June 17). Disaster Recovery Planning: Untapped Success Factor in an Organization. SSRN. Retrieved December 4, 2020, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3628630

Cloud Computing - Myths and Realities. (2014, February 19). Communications Today.

Graves, B. (2017, August 14). The myths of cloud computing: figuring out the true costs, risks and complexities of the cloud. San Diego Business Journal, 38(33), 15+.

Cloud Computing & Data Backup

LogFire Dispels Top Supply Chain Cloud Computing Myths. (2012, September). Supply & Demand Chain Executive.