Semba Wijaya | SIB 4C | KSI

Lab - Recommend Disaster Recovery Measures

Objectives

Part 1: Natural Disaster

Part 2: DDoS Attack

Part 3: Loss of Data

Background / Scenario

Every organization needs to be prepared for a disaster. The ability to recover from a disaster can determine the survival of the business. A disaster can be a hurricane or typhoon, hardware failure, loss of data, or a devastating cyber attack.

A disaster recovery plan will include policies and procedures that the organization follows when IT services are disrupted.

In the plan, you should take into account IT-related people, services and equipment, and the physical locations of the business. You should also keep in mind of recovery point objectives (RPO) and recovery time objectives (RTO).

In this lab, you will recommend disaster recovery measures for a natural disaster, equipment failure in the datacenter, a DDoS attack, or loss of data for a tutoring service.

In this business, you have students from different geographical locations who require tutoring for different subjects, such as mathematics and language. The students have access to an online curriculum that provides them with supplemental materials based on their needs. The students can also sign up for personal assistance from instructors for scheduled small group or one-to-one tutoring services. The business has a few physical locations that potential customers can visit and use the tutoring services in-person. The business delivers services to its customers from a neighboring cloud data center. The data center delivers instructional content, student records, registration for services, and real-time video conferencing for direct instruction. Other routing business practices, such as backups of onsite business servers is handled in the data center.

Required Resources

- Device with internet access

Instructions

Part 1: Natural Disaster

A hurricane, or typhoon, has struck your community and caused damage near a data center. The network infrastructure in the area has also suffered damage.

The damage near the data center has caused a network outage and the servers in the data center are no longer accessible remotely. Because of the extensive damage in the community, it may take a few days before a thorough damage assessment can be completed. You can assume that there is no access to this data center for at least a week.

Step 1: Identify the potential risks.

Questions:

Answer the following questions:

Can the business operate without access to this data center? Explain.

Answer Area

The business will have limited functions at the physical locations only. The business requires access to the servers within the data center remotely. Without them, the business cannot function because customers cannot access the tutoring services and the online content. Furthermore, instructors cannot provide tutoring and cannot access student information remotely. Additionally, the inability to utilize the online curriculum may lead to decreased student satisfaction and potential loss of clients during this outage.

Can the students access their online materials? Explain.

Answer Area

The students will not be able to access the online materials if all the materials are located in the same inaccessible data center. This lack of access may hinder their learning progress and lead to frustration, as they depend on these materials for their studies. If alternative resources are not provided, the students may seek other tutoring options, impacting the business's reputation.

Are there other ways that instructors can provide the tutoring services? Explain.

Answer Area

The instructors can still provide services if they can connect with students via meeting applications that are provided by other online providers. If the instructors have access to their teaching materials stored locally or on personal devices, they could continue delivering lessons through these platforms, mitigating the impact of the disaster on student learning.

Can new users sign up for the tutoring services? Explain.

Answer Area

New users cannot use the service if they cannot access the business's online user database that is housed in the inaccessible data center. This restriction not only affects new sign-ups but also limits the business's growth potential and market reach during the recovery period.

Can the employees access internal company information during the recovery?

Answer Area

The employees cannot access internal information if the internal servers are also located at the same data center. This lack of access may delay decision-making processes and hinder operational efficiency. Employees may need to rely on alternative methods for communication and updates regarding the recovery efforts.

Step 2: Recommend a disaster recovery plan.

Based on your answers in the previous step, list your recommendations below:

Answer Area

This business cannot function successfully without access to its user database and online curriculum. A backup location should house an up-to-date backup copy of the essential data. In the event that the current data center is inaccessible, a backup location should come online and provide the essential services.

- Current backup copy of the user database and online curriculum
- Secondary physical location with a different ISP to ensure connectivity
- Backup location should be available in a short period of time during recovery
- Internal server access for employees for updated information during recovery
- Each employee should have a local copy of the disaster recovery plan to ensure everyone is informed and can act quickly
- Regular training and simulations for staff to prepare them for potential disasters

Part 2: DDoS Attack

A few users have reported that they cannot log into their accounts and access the online curriculum. Upon further investigation, it appears that the web server is overwhelmed with requests at a time when normally there is little traffic. It appears that the server is undergoing a denial of service attack.

Step 1: Identify potential problems.

questions:

Answer the following questions:

Can the business operate without access to data center? Explain.

Answer Area

The business requires access to the servers within the data center remotely. Without access, the business cannot function because customers cannot access the tutoring services and the online content. In addition, instructors cannot provide tutoring or access student information. This situation could lead to significant operational disruptions and financial losses for the business.

Can the business still function without access to the data center? Explain.

Answer Area

The business has limited function if only the staffed physical locations can provide the tutoring services. If instructors are available, they can offer in-person sessions, but this is contingent on the number of students who can physically attend the locations.

Can the students access their online materials? Explain.

Answer Area

The students cannot access their online materials because access to the servers at the data center is not available. Without these materials, students may feel unprepared for their classes, which could impact their academic performance and retention rates.

Can the instructors still provide the tutoring services? Explain.

Answer Area

The instructors can still provide services if they can connect with their students via meeting applications that are provided by other online providers. However, the effectiveness of these sessions may be limited without access to the core instructional materials and curriculum.

Can new users sign up for the tutoring services? Explain.

Answer Area

New users cannot use the service if they cannot access the business's online user database or curriculum. This limitation could hinder the organization's ability to attract new clients and grow during the downtime.

Can the employees access internal company information during the recovery?

Answer Area

The employees have no access to internal information during recovery. This could lead to delays in resolving issues and implementing solutions, as key personnel may not have the necessary information to proceed effectively.

Step 2: Recommend a recovery plan.

Based on your answers in the previous step, list your recommendations below:

Answer Area

This business cannot function without access to its user database and online curriculum. In the event of an attack:

- Current backup copy of the user database, online curriculum at a different physical location
- Backup copies of the servers that can be deployed as needed to minimize downtime

- Each employee should have a local copy of the disaster recovery plan to ensure clarity in action steps

- Identification and testing of alternate communication services to those housed in the data center
- Establishing monitoring systems to detect unusual traffic patterns that could indicate future DDoS attacks

Part 3: Loss of Data

Users have reported that they are unable to login to their accounts, and they were unable to reset their credentials. Other users have reported that they were able to log in, but their recent progress in their classes is missing. After further investigation, it appears that the data loss was caused by human error.

Step 1: Identify potential problems.

questions:

Answer the following questions:

Can the business operate with the data loss? Explain.

Answer Area

It depends on the extent of data loss. The business should be able to continue with possible limitations, particularly if critical data like user accounts and progress records have been compromised. This can lead to dissatisfaction among students and potential churn.

Can the students access their online materials? Explain.

Answer Area

The students can only access their online materials if their online materials are not part of the lost data and their accounts can be restored. If significant data has been lost, it could create a gap in students' learning experiences.

Can the instructors still provide the tutoring services? Explain.

Answer Area

The instructors can only access their online materials if their online materials are not part of the lost data. This can limit their ability to deliver effective tutoring sessions, potentially affecting student learning outcomes.

Can new users sign up for the tutoring services? Explain.

Answer Area

New users can sign up if they are not accessing the business's online user database or curriculum that is part of the data loss. However, if sign-up processes depend on the same compromised systems, this may not be possible, affecting the organization's growth.

Can the employees access internal company information during the recovery?

Answer Area

The employees have access to internal information during recovery if it is not part of the data loss. This access is crucial for the continuation of operations and effective recovery efforts.

Step 2: Recommend a recovery plan.

Based on your answers in the previous step, list your recommendations below:

Answer Area

The business should have daily backups of all essential data, such as the user database. Multiple backups of the data at different time increments may be necessary because the undamaged data could be in an older backup only.

For example, if the data was damaged by the insertion of malicious code by an attacker two days ago, and the company keeps full daily backups for seven days, the damaged data can be recovered from the backup that is three days old. However, the trade-off for using an older backup is losing the data from the last two days. Conversely, if the damaged data can be identified and recovered from the backups, the data loss can be minimized if only the damaged data is incrementally replaced from the backups.

Furthermore, software vulnerability and malicious attacks can also cause data loss in addition to human errors and sabotage.

- Retain multiple copies of the backups taken at different time intervals for added security
- Implement anti-malware software to prevent potential data loss threats
- Keep software up-to-date to safeguard against vulnerabilities
- Each employee should have a local copy of the disaster recovery plan to ensure they are prepared
- Rapid data restore capability on redundant equipment to minimize downtime during recovery

Reflection

1. **These cases indicate disaster recovery requirements that are common to many businesses that use offsite datacenters. What should be included disaster recovery plans for many of these business?**

Answer Area

One thing that is very important is that essential data operations be housed offsite in a data center. Because that data center could become unreachable, servers should mirror data between two or more data centers. In this way, virtual servers can be created at the backup data center so that business operations can be restored as quickly as possible. Additionally, it’s

crucial to have a comprehensive risk assessment process to identify potential vulnerabilities and impacts. Of additional importance, because the most current backup may not include damaged or lost

data, backups should be archived for some period to allow for restoration from the last good backup.

2. **Now that you have examined a few scenarios and provided some possible disaster recovery measures, what other actionable recommendations are essential for a successful disaster recovery?**

Answer Area

For a recovery plan to be successful, responsible individuals should be assigned to lead the recovery process and perform the recovery measures. The plan should be tested regularly if possible, and all employees should be trained in the recovery process to know what to do in the event of a disaster. The plan should be accessible to all employees and be updated as necessary, taking into account lessons learned from past incidents. Additionally, fostering a culture of preparedness and awareness throughout the organization can significantly enhance the effectiveness of the disaster recovery plan.