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.

Answer the following questions:

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

Answer: The business will have limited functions at physical locations only. Access to the servers within the data center is essential for the business to operate as customers cannot access tutoring services and online content. Instructors also need access to student information to provide tutoring.

Answers will vary. 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 the customers cannot access the tutoring services and the online content. Furthermore, the instructors cannot provide tutoring and cannot access the student information remotely.

Can the students access their online materials? Explain.

Answer: No, students cannot access online materials if all content is housed in the inaccessible data center.

Answers will vary. The students will not be able to access the online materials if all the materials are located in the same inaccessible data center.

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

Answer: Yes, instructors can utilize meeting applications provided by third-party platforms (e.g., Zoom, Google Meet) if they can connect with students independently.

Answers will vary. The instructors can still provide services if they can connect with students via meeting applications that are provided by other online providers.

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

Answer: No, new users cannot sign up as they require access to the online user database housed in the data center.

Answers will vary. New users cannot use the service if they cannot access the business's online user database that is housed in the inaccessible data center.

Can the employees access internal company information during the recovery?

Answer: No, employees cannot access internal information if all servers are located in the inaccessible data center.

Answers will vary. The employees cannot access internal information if the internal servers are also located at the same data center.

Step 2: Recommend a disaster recovery plan.

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

Answer:

- Establish a backup location that houses an up-to-date copy of essential data.
- Ensure there is a secondary physical location with a different ISP to mitigate risks.
- The backup location should be operational within a short recovery timeframe.
- Provide internal server access for employees to retrieve updated information during recovery.
- Distribute a local copy of the disaster recovery plan to each employee.

Answers will vary. This business cannot function successfully without access 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**
- **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 disaster recovery plan**

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.

Answer the following questions:

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

Answer: No, the business cannot fully function without access as it requires servers in the data center for all operations.

Answers will vary. 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.

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

Answer: The business can only provide limited services from physical locations if online services are down.

Answers will vary. The business has limited function if only the staffed physical locations can provide the tutoring services.

Can the students access their online materials? Explain.

Answer: No, students cannot access their materials if the data center is overwhelmed and services are unavailable.

Answers will vary. The students cannot access their online materials because access to the servers at the data center is not available.

Can the instructors still provide the tutoring services? Explain.

Answer: Yes, instructors can provide tutoring through alternative platforms if they can connect with students outside the affected infrastructure.

Answers will vary. The instructors can still provide services if they can connect with their students via meeting applications that are provided by other online providers.

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

Answer: No, without access to the online user database, new users cannot sign up.

Answers will vary. New users cannot use the service if they cannot access the business's online user database or curriculum.

Can the employees access internal company information during the recovery?

Answer: No, if the internal servers are also affected, employees will lack access to necessary information.

Answers will vary. The employees have no access to internal information during recovery.

Step 2: Recommend a recovery plan.

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

Answer:

- Maintain a current backup of the user database and online curriculum at a different physical location.
- Ensure backup copies of servers are available to deploy as needed.
- Provide each employee with a local copy of the disaster recovery plan.
- Identify and test alternative communication services to those housed in the data center.

Answers will vary. 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**
- **Each employee should have a local copy of disaster recovery plan**
- **Identification and testing of alternate communicate services to those housed in the data center**

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.

Answer the following questions:

Can the business operate with the data loss? Explain.

Answer: It depends on the extent of data loss. The business may continue with some limitations if critical data is recoverable.

Answers will vary. It depends on the extent of data loss. The business should be able to continue with possible limitations.

Can the students access their online materials? Explain.

Answer: Yes, students can access their materials if they are not part of the lost data and their accounts can be restored.

Answers will vary. 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.

Can the instructors still provide the tutoring services? Explain.

Answer: Instructors can continue providing tutoring if their required materials are intact and accessible.

Answers will vary. The instructors can only access their online materials if their online materials are not part of the lost data.

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

Answer: New users can sign up if the online user database is unaffected by data loss.

Answers will vary. New users can sign up if they are not accessing the business's online user database or curriculum that is part of data loss.

Can the employees access internal company information during the recovery?

Answer: Employees can access internal information during recovery as long as it is not part of the lost data.

Answers will vary. The employees have access to internal information during recovery if it is not part of the data loss.

Step 2: Recommend a recovery plan.

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

Answer:

- Implement daily backups of essential data, including the user database.
- Maintain multiple backups at different time increments to mitigate data loss risks.
- Use anti-malware software and ensure software is regularly updated.
- Provide rapid data restore capabilities on redundant equipment.
- Distribute a local copy of the disaster recovery plan to each employee.

Answers will vary. The business should have daily backups of all the 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, the data was damaged by the insertion of malicious code by an attacker 2 days ago. The company keeps full daily backups for seven days. The damaged data can be recovered from the backup that this is 3 days old. However, the trade-off for using an older backup is losing the data from the last two days. On the other hand, 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**
- **Anti-malware software**
- **Keep software up-to-date**
- **Each employee should have a local copy of disaster recovery plan**
- **Rapid data restore capability on redundant equipment**

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?

   Essential data operations should be housed offsite. Data mirroring between multiple data centers allows quick restoration of operations. Regular archiving of backups ensures that the most recent and unaffected data can be restored when necessary.

   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, server 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. Of additional importance, because the most current backup may not include damaged or last data that backups be archived for some period of time, so that the last good backup can be restored.

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?

   Assign responsible individuals to lead the recovery process. The recovery plan should be regularly tested, and employees must be trained in the recovery processes. Ensure the plan is easily accessible to all employees and is updated as needed.

   Answers will vary. 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 if possible and all the employees should be trained in the recovery process and know what to do in the event of a disaster. The plan should be available for all the employees and be updated as necessary.