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

TASK 1

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:

QUESTION 1

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

I don’t think business can operate without access to this data center if the functions and operations of the business is dependent on this data center specifically for their day to day operation.

QUESTION 2

Can the students access their online materials? Explain.

No, the students might have problem if the online materials were remotely stored in this data center and not elsewhere.

QUESTION 3

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

The instructors can provide the tutoring services if they can connect with students through other third-party platforms while their business focuses on recovering the files on this data center.

QUESTION 4

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

New users cannot use the service if they cannot access the business’s online user database that is housed in the inaccessible data centre.

QUESTION 5

Can the employees access internal company information during the recovery?

The employees cannot access internal information if the internal servers are also located at the same data centre.

Step 2: Recommend a disaster recovery plan.

QUESTION 6

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

- 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

TASK 2

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:

QUESTION 1

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

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.

QUESTION 2

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

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

QUESTION 3

Can the students access their online materials? Explain.

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

QUESTION 4

Can the instructors still provide the tutoring services? Explain.

The instructors can provide the tutoring services if they can connect with students through other third party platforms.

QUESTION 5

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

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

QUESTION 6

Can the employees access internal company information during the recovery?

The employees have no access to internal information during recovery.

Step 2: Recommend a recovery plan.

QUESTION 7

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

- Implement Web Application Firewall (WAF) to filter malicious traffic.
- Use DDoS protection services like Cloudflare, AWS Shield, or Akamai.
- Create an incident response plan specifically for DDoS scenarios.
- Set up alerts and logs for suspicious or unusual traffic patterns.
- Keep backups for data recovery

TASK 3

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:

QUESTION 1

Can the business operate with the data loss? Explain.

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

QUESTION 2

Can the students access their online materials? Explain.

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

QUESTION 3

Can the instructors still provide the tutoring services? Explain.

They can provide the tutoring services manually but might be difficult because necessary required might be lost.

QUESTION 4

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

New users may not be able to sign up if the registration system or user database is affected.

QUESTION 5

Can the employees access internal company information during the recovery?

Employees may have limited access depending on which systems or databases are affected by the data loss.

Step 2: Recommend a recovery plan.

QUESTION 6

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

- Restore from most recent backup to recover lost data.
- Anti-malware software
- Keep software up-to-date
- Retain multiple copies of the backups taken at different time intervals

TASK 4

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

   A comprehensive disaster recovery plan for businesses utilizing offsite datacenters should include a risk assessment, robust data backup and replication strategies, the establishment of a secure disaster recovery site with appropriate redundancy, clear recovery objectives (RTO and RPO), a detailed communication plan, and defined roles and responsibilities for the disaster recovery team, along with regular testing and updates.

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

   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.