Nama : Winda Umi Fatimatus Sa’diyah

NIM : 2141762055

Absen : 19

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 inperson. 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:

- No, the business will have limited operations restricted to physical locations only. Remote access to servers is essential for full functionality, especially for online tutoring services and remote access to student records.

Can the students access their online materials? Explain.

- No, students will not be able to access their online materials if the materials are stored solely in the inaccessible data center.

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

- Yes, instructors can provide tutoring using external meeting applications and platforms if they have the ability to connect with students outside the main data center infrastructure.

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

- No, new users cannot register if access to the online user database and necessary infrastructure is unavailable.

Can the employees access internal company information during the recovery?

- No, employees will not be able to access internal company information if the servers hosting this data are located in the affected data center.

Step 2: Recommend a disaster recovery plan.

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

- Maintain a backup copy of essential data (user database and online curriculum) at a secondary location.
- Establish a secondary location with a different ISP for redundancy.
- Ensure the backup site is configured for rapid deployment during disaster recovery.
- Employees should have a local copy of the disaster recovery plan and be trained in its use.
- Implement remote access for essential company information stored on backup servers.

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.

- No, without access, the business will have significant operational issues as customers cannot access services and instructors cannot access student data.

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

- Limited functionality may exist through staffed physical locations that can offer services directly.

Can the students access their online materials? Explain.

- No, students will not be able to access materials stored on servers within the affected data center.

Can the instructors still provide the tutoring services? Explain.

- Yes, if they can use third-party meeting applications to connect with students, some tutoring can continue.

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

- No, new users will not be able to sign up if they cannot access the database or online curriculum.

Can the employees access internal company information during the recovery?

- No, access to internal information will be limited if it is hosted at the affected data center.

Step 2: Recommend a recovery plan.

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

- Maintain a current backup copy of the user database and online curriculum at an alternate location.
- Have backup servers ready for deployment as needed.
- Distribute local copies of the disaster recovery plan to employees.
- Test and identify alternative communication platforms that can be used if the primary data center is compromised.

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.

- It depends on the extent of the loss. Limited operations may continue, but there could be significant disruptions.

Can the students access their online materials? Explain.

- Students can access materials only if those resources are not part of the lost data and can be restored.

Can the instructors still provide the tutoring services? Explain.

- Yes, if their materials and necessary data have not been lost.

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

- New user registrations may be impacted if the user database or other critical data is lost.

Can the employees access internal company information during the recovery?

- Employees may be limited in their access if critical data related to internal operations is affected.

Step 2: Recommend a recovery plan.

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

- Ensure daily backups of essential data, including the user database.
- Maintain multiple backup copies taken at different intervals to protect against data corruption.
- Use anti-malware and keep software updated to minimize risks.
- Provide employees with local copies of the recovery plan.
- Implement rapid data restoration capabilities and redundant equipment for seamless data 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?

   - Include mirrored data between multiple data centers to ensure that business operations can be restored quickly.
   - Archive backups for a sufficient period to ensure the last good backup can be used if needed.

- Use automated failover systems for rapid recovery.

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 dedicated recovery leaders to oversee the process.
   - Conduct regular tests of the disaster recovery plan.
   - Train all employees on recovery protocols to ensure preparedness.

   Keep the recovery plan up to date and easily accessible