Rossi Dea Agatha
SIB 4C – 2141762112

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.

Answer the following questions:

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

- No, the business can only provide limited services at physical locations. Remote access to the data center is essential for customer access to tutoring services, online content, and for instructors to access student information. Without it, most business functions are halted.

Can the students access their online materials? Explain.

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

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

- Yes, if instructors have access to alternative online meeting tools (e.g., Zoom, Google Meet), they can still connect with students for remote sessions, although it may be limited compared to the full curriculum platform.

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

- No, new user registrations rely on access to the user database, which is unavailable if housed in the data center.

Can the employees access internal company information during the recovery?

- No, employees will not have access to internal information if internal servers are hosted in the inaccessible data center.

Step 2: Recommend a disaster recovery plan.

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

- Maintain an up-to-date backup copy of the user database and online curriculum in a secondary location.
- Establish a secondary physical location with a different ISP to avoid network outages in a single area.
- Ensure the backup location is quickly accessible to minimize downtime.
- Provide internal server access for employees to stay updated during recovery.
- Distribute a local copy of the disaster recovery plan to each employee.

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.

- No, the business requires access to its data center for online tutoring services, curriculum, and student information.

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

- Limited functionality may be possible, but only in physical locations without full online capabilities.

Can the students access their online materials? Explain.

- No, if the data center is overwhelmed by the attack, students cannot access their online curriculum.

Can the instructors still provide the tutoring services? Explain.

- Yes, instructors can still use other online meeting tools (e.g., Zoom, Google Meet) to conduct tutoring sessions, though they won't have access to all online materials.

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

- No, registration is impossible without access to the online user database and curriculum.

Can the employees access internal company information during the recovery?

- No, employees will not have access to internal information without data center connectivity.

Step 2: Recommend a recovery plan.

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

- Store backup copies of the user database and online curriculum at a secondary physical location.
- Prepare deployable backup server copies as needed.
- Distribute a local copy of the disaster recovery plan to each employee.
- Identify and test alternative communication methods outside of the primary 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.

- It depends on the extent of the data loss. The business might operate with some limitations, but critical data loss could hinder functions.

Can the students access their online materials? Explain.

- Only if their data and access credentials are unaffected by the loss.

Can the instructors still provide the tutoring services? Explain.

- Yes, as long as the essential instructional data they need hasn't been lost.

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

- New users can sign up if the data loss does not include the parts of the user database required for registration.

Can the employees access internal company information during the recovery?

- If the internal information is unaffected by the data loss, employees will retain access.

Step 2: Recommend a recovery plan.

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

- Implement daily backups of essential data, such as the user database, to minimize the impact of data loss.
- Store multiple backup copies from different time points to ensure a viable backup remains available.
- Employ anti-malware software and maintain updated security software to protect against further incidents.
- Provide a local copy of the disaster recovery plan to each employee.
- Enable rapid data restoration 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 operations should be housed offsite with mirrored data across multiple data centers. Virtual servers should be configured for fast restoration, with multiple backup versions stored over time to avoid corrupted or lost data. Archiving past backups also allows restoration from the last stable version.

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. Regularly test the recovery plan, provide training to employees, and ensure the plan is easily accessible to all employees. Update the plan as necessary to adapt to new technologies or potential risk.