Nama : Sasmita Rachmawati

Absen : 15

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: No, the business will be severely limited without the data center, as access to essential online materials and student records is required. Without the remote servers, students and instructors cannot access curriculum materials, and tutoring services cannot function.

Can the students access their online materials? Explain.

Answer: No, students will not be able to access online materials if those materials are located only within the inaccessible data center.

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

Answer : Yes, instructors may use other online meeting platforms (e.g., Zoom or Google Meet) for tutoring sessions, assuming students can access those platforms independently.

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

Answer: No, new sign-ups would be restricted if access to the database or registration system is only available in the affected data center.

Can the employees access internal company information during the recovery?

Answer: No, if internal servers are also in the data center, employees cannot access internal information without remote access.

Step 2: Recommend a disaster recovery plan.

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

Answer:

1. **Secondary Backup Location: Establish a backup data center in a geographically separate location to allow critical operations to resume during disasters.**
2. **Data Backups: Maintain current backups of essential data such as user databases and curriculum, stored at the backup data center.**
3. **Network Redundancy: Use a different ISP for the backup location to maintain connectivity.**
4. **Local Copy of Disaster Plan: Each employee should have a local copy of the disaster recovery plan.**

5. **Employee Access to Internal Servers: Ensure internal access for employees to retrieve essential information.**

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: No, the business depends on the data center for tutoring services and content delivery, and without access, services would be severely impacted.

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

Answer: No, the business can only function in a limited capacity without access to the data center. Physical locations may still provide some in-person tutoring, but essential online components like curriculum access, student records, and remote tutoring are unavailable.

Can the students access their online materials? Explain.

Answer: No, students cannot access materials if the data center servers are overwhelmed by the attack.

Can the instructors still provide the tutoring services? Explain.

Answer: Yes, if instructors use alternative online meeting platforms not affected by the DDoS attack.

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

Answer: No, new users cannot register if access to the database is disrupted by the attack.

Can the employees access internal company information during the recovery?

Answer: No, without access to the data center, employees cannot retrieve internal information.

Step 2: Recommend a recovery plan.

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

Answer:

1. **Alternate Location for Backup Data: Have a backup data center where a copy of the user database and curriculum is stored.**
2. **DDoS Mitigation: Use DDoS protection services or alternate servers for essential services.**
3. **Disaster Plan Copy for Each Employee: Ensure all employees have a local disaster recovery plan.**
4. **Communication Alternatives: Use non-impacted online communication services if needed.**

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: Partially; operations depend on the extent of data loss. If core data like student records is missing, functions may be limited.

Can the students access their online materials? Explain.

Answer: Yes, if their data was not affected. Otherwise, they may face issues accessing course materials.

Can the instructors still provide the tutoring services? Explain.

Answer: Yes, as long as essential resources are unaffected, but data integrity issues could limit effectiveness.

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

Answer: Yes, if registration data and systems remain intact and are unaffected by data loss.

Can the employees access internal company information during the recovery?

Answer: Yes, if the required data is accessible and unaffected by the loss.

Step 2: Recommend a recovery plan.

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

Answer:

1. **Daily Backups: Store daily backups of essential data across different intervals to recover the latest intact version.**
2. **Anti-Malware Software: Protect systems to prevent data loss due to malware.**

3. **Redundant Data Restore Capability: Have equipment capable of restoring data from backups rapidly.**
4. **Employee Copies of the Disaster Recovery Plan: Ensure employees have access to updated versions of the plan.**

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: Data operations should be housed across multiple data centers with mirrored servers to allow for rapid recovery. A mirrored setup enables backup data centers to activate virtual servers to restore operations quickly. Maintain older backups for data integrity in case recent backups contain corrupted or damaged data.

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: Assign specific roles for recovery processes, and train employees on recovery procedures. Regularly test and update the plan, and ensure it is accessible to all employees in case of an emergency.