Nama : Yusufa Haidar

Kelas : SIB – 4C

Absen : 21

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.

The business will have limited functions at physical locations only. The remote access to servers within the data center is critical for operations. Without this access, the business cannot function effectively because customers cannot access the tutoring services or the online content. Furthermore, instructors cannot provide tutoring or access student information remotely, severely impacting the business's core activities.

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.

If all the online materials are housed within the inaccessible data center, students will not be able to access these materials. The lack of access means that any coursework, assignments, or resources stored in that data center are also out of reach.

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.

Instructors can potentially provide services using alternative meeting applications provided by other online providers. They can use tools like Zoom, Microsoft Teams, or Google Meet to connect with students, provided they have access to necessary materials and student information.

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.

New users cannot sign up if the business’s online user database is housed in the inaccessible data center. The inability to access the database means that registration and onboarding processes for new users are halted.

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

Can the employees access internal company information during the recovery?

Employees cannot access internal information if the internal servers are also located in the same data center. This includes any documents, communications, and resources stored on those servers, impeding the ability to perform day-to-day tasks.

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:

1. **Implement Redundant Data Centers:**
    - Establish a secondary data center in a geographically different location to ensure that operations can continue if one data center becomes inaccessible. This would allow for failover in case of a di saster affecting one location.
2. **Cloud-Based Solutions:**

- Transition critical services to cloud-
  based platforms which can provide high availability and disaster recovery capabilities. This would allow students to access materials and instructors to provide services even when physical data ce nters are down.

3. **Backup and Disaster Recovery Plans:**
   - Regularly backup all critical data and ensure that backup data is stored offsite or in the cloud. Tes t disaster recovery plans to ensure they can be executed quickly and effectively in an emergency.
4. **Alternative Communication Platforms:**
   - Train instructors to use alternative communication platforms like Zoom, Microsoft Teams, or Goog le Meet to continue providing tutoring services in the event that internal systems are inaccessible.
5. **Enhanced Physical Security:**
   - Improve physical security measures to prevent unauthorized access to critical infrastructure. This includes security cameras, access control systems, and security personnel.
6. **Employee Training:**
   - Conduct regular training for employees on emergency response procedures, including how to con tinue operations without access to the primary data center and how to use alternative platforms ef fectively.
7. **Develop a Contingency Plan:**
   - Create a detailed contingency plan that outlines steps to take in the event of a prolonged data ce nter outage, ensuring all employees are familiar with their roles and responsibilities.
8. **External MSSP Coordination:**
   - Maintain close coordination with the managed security service provider (MSSP) to ensure 24/7 m onitoring and rapid response in case of any security incidents during the recovery period.

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.

â€¢ Current backup copy of the user database and online curriculum
â€¢ Secondary physical location with a different ISP
â€¢ Backup location should be available in a short period of time during recovery
â€¢ Internal server access for employees for updated information during recovery
â€¢ 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.

The business requires remote access to the servers within the data center to function. Without this access, customers cannot access tutoring services or online content, and instructors cannot provide tutoring or access student information. Consequently, the business cannot function effectively.

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.

The business has limited functionality if only the staffed physical locations can provide tutoring services. However, this is not a sustainable solution as the primary mode of operation relies on remote access to services hosted in the data center.

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.

Students cannot access their online materials if all the materials are stored on servers in the inaccessible data center. This disrupts their learning process as they rely on these materials for their coursework.

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.

Instructors can still provide services if they can connect with their students via meeting applications provided by other online providers (like Zoom, Microsoft Teams, or Google Meet). However, they would need access to the required teaching materials and student information.

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.

New users cannot sign up for the tutoring services if they cannot access the business's online user database or curriculum stored in the data center. The sign-up process relies on this data to onboard new users.

Answers will vary. New users cannot use the service if they cannot access the businessâ€™s online user database or curriculum.

Can the employees access internal company information during the recovery?

Employees cannot access internal company information if it is stored on servers located in the same inaccessible data center. This hampers their ability to perform administrative and operational tasks.

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:

1. **Implement Redundant Data Centers:**
    - Establish a secondary data center in a different geographical location to ensure operations can co ntinue if one data center becomes inaccessible. This would provide failover capabilities in case of an attack.
2. **Cloud-Based Solutions:**
    - Transition critical services to cloud-based platforms that offer high availability and built in DDoS protection. This would allow students to access materials and instructors to provide services even if physical data centers are down.
3. **Enhanced DDoS Protection:**
    - Utilize DDoS protection services from providers like Cloudflare or AWS Shield to mitigate the impact of DDoS attacks and ensure that the web servers remain accessible.
4. **Backup and Disaster Recovery Plans:**

- Regularly backup all critical data and ensure that backups are stored offsite or in the cloud. Test disaster recovery plans to ensure quick and effective execution in emergencies.

5. **Alternative Communication Platforms:**
    - Train instructors to use alternative communication platforms like Zoom, Microsoft Teams, or Google Meet to continue providing tutoring services during outages.
6. **Scalable Infrastructure:**
    - Implement scalable infrastructure that can handle sudden spikes in traffic, helping to absorb and mitigate DDoS attacks.
7. **Improved Security Training:**
    - Conduct regular training for employees on how to recognize and respond to DDoS attacks and other security incidents.
8. **Load Balancers and Traffic Filtering:**
    - Use load balancers and traffic filtering solutions to distribute traffic evenly across servers and filter out malicious traffic.
9. **Incident Response Plan:**
    - Develop and regularly update an incident response plan specifically for DDoS attacks, ensuring all employees are familiar with their roles and responsibilities during an attack.
10. **MSSP Coordination:**

- Maintain close coordination with the managed security service provider (MSSP) for 24/7 monitoring and rapid response to DDoS attacks and other security incidents.

Answers will vary. This business cannot function without access to its user database and online curriculum. In the event of an attack:

â€¢ Current backup copy of the user database, online curriculum at a different physical location
â€¢ Backup copies of the servers that can be deployed as needed
â€¢ Each employee should have a local copy of disaster recovery plan
â€¢ 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.

It depends on the extent of the data loss. If the lost data includes critical operational information, the business may face significant disruptions. However, if the impact is limited, the business can continue with some limitations, possibly affecting service delivery and customer satisfaction.

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.

Students can only access their online materials if those materials are not part of the lost data and their accounts can be restored. If the lost data includes crucial educational resources, students' access will be disrupted until the data is recovered.

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.

Instructors can only provide tutoring services if their access to online materials and student information is not affected by the data loss. If these resources are part of the lost data, instructors will face challenges in delivering effective tutoring services.

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.

New users can sign up if the data loss does not affect the business's online user database or curriculum. If these components are impacted, new user registrations will be hindered until the data is restored.

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

Can the employees access internal company information during the recovery?

Employees can access internal information during recovery if it is not part of the data loss. If essential internal data is lost, employees' ability to perform their roles will be limited until data recovery is complete.

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:

1. **Regular Data Backups:**
    - Schedule frequent and consistent backups of all critical data. Ensure these backups are stored in secure, offsite locations or in the cloud to provide resilience against data loss incidents.
2. **Data Recovery Plan:**
    - Develop and rigorously test a comprehensive data recovery plan to ensure swift restoration of lost data. This plan should include detailed procedures for different types of data loss scenarios.
3. **Enhanced Access Controls:**
    - Implement strict access controls and permissions to minimize the risk of human error leading to data loss. Limit access to critical systems and data only to authorized personnel.
4. **Employee Training:**
    - Conduct regular training sessions for employees on data handling best practices and the importance of data integrity. Emphasize the role each employee plays in preventing data loss and maintaining security.
5. **Automated Backup Solutions:**
    - Utilize automated backup solutions to ensure that data backups are consistently performed without relying on manual intervention. Automated systems can reduce the risk of oversight and ensure regular backup schedules are maintained.
6. **Version Control Systems:**
    - Implement version control systems for key documents and data, allowing for rollback to previous versions in case of accidental data loss or corruption.
7. **Incident Response Team:**

- Establish a dedicated incident response team trained to handle data loss incidents efficiently. Ensure that this team has clear protocols and communication strategies in place.

8. **Regular Audits and Monitoring:**
    - Conduct regular audits of data handling processes and monitor for any anomalies that might indicate potential data loss. Use monitoring tools to detect and respond to data integrity issues promptly.

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.

â€¢ Retain multiple copies of the backups taken at different time intervals
â€¢ Anti-malware software
â€¢ Keep software up-to-date
â€¢ Each employee should have a local copy of disaster recovery plan
â€¢ 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 Offsite:** Ensure that critical data operations are housed in an offsite data center. Given the risk of the data center becoming unreachable, it's crucial to mirror data between two or more data centers.
    - **Data Mirroring:** Implement data mirroring to allow virtual servers to be created at a backup data center. This ensures that business operations can be quickly restored.
    - **Backup Archives:** Maintain archives of backups for a period of time. This is important because the most recent backup may include corrupted or lost data. Archived backups allow for restoration of the last good backup.

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?

   - **Assignment of Responsible Individuals:** Assign dedicated individuals to lead the recovery process and execute recovery measures effectively.
   - **Testing the Plan:** Regularly test the disaster recovery plan to identify and address any weaknesses. Simulated disaster recovery drills can help in preparedness.
   - **Employee Training:** Train all employees on the recovery process and their specific roles in the event of a disaster. This ensures everyone knows what to do and can respond quickly.
   - **Plan Accessibility and Updates:** Make the recovery plan readily accessible to all employees. Regularly update the plan to reflect any changes in the business operations or infrastructure.

   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.