DISASTER RECOVERY ASSESSMENT REPORT

-Group 26

EXECUTIVE SUMMARY

The Disaster Recovery Assessment of our AWS cloud environment has provided crucial insights into our preparedness for unforeseen disruptions. The assessment highlighted the absence of a comprehensive backup and disaster recovery plan, potentially exposing us to data loss and extended downtime in disaster scenarios. The lack of snapshots for virtual machine instances was also identified as a challenge, making recovery more challenging after successful cyberattacks or system failures. In light of these findings, it is imperative that we establish robust backup and recovery strategies, automate snapshot creation, define clear retention policies, and conduct regular testing to ensure the resilience of our AWS cloud environment. These measures will not only enhance our disaster recovery capabilities but also safeguard business continuity in the face of unexpected challenges.

INTRODUCTION

In this disaster recovery assessment report, the cloud infrastructure for the healthcare organization is assessed with a particular emphasis on its capacity for disaster recovery. It is crucial to guarantee these cloud resources' security and availability in the case of emergencies or disruptions. In order to preserve patient data protection and the ongoing provision of healthcare services, this disaster recovery assessment study seeks to examine the level of disaster recovery readiness within our healthcare cloud infrastructure and pinpoint areas that require improvement.

SCOPE

This assessment's scope includes all cloud-based systems, apps, and resources that are essential to the provision of healthcare services. It will assess the efficiency of the present disaster recovery plans, testing procedures, and adherence to laws unique to the healthcare industry, like HIPAA. The evaluation will also look at how ready our cloud infrastructure is to handle other types of emergencies, such as cyberattacks, natural catastrophes, and unplanned system outages. This report's conclusions and suggestions will act as a cornerstone for enhancing our healthcare cloud environment's disaster recovery capabilities.

IDENTIFIED RISKS OF DATA LOSS AND EXTENDED DOWNTIME

Improper Log handling.

First, it could result in inaccurate or missing security event data, which would make it more difficult to identify and handle security incidents. Because flow logs must be retained and analyzed for regulatory purposes, improper log handling can also lead to excessive storage costs and difficulties with compliance and audits. Finally, if logs containing personally identifiable or confidential data are not properly secured or redacted, raising the possibility of data leakage, improper flow log handling may expose sensitive information and violate privacy.

No Multi-Factor Authentication mechanisms in place.

Since a password serves as the sole authentication requirement in the absence of multifactor authentication, user accounts are more susceptible to unauthorized access. This risk also includes the possibility of data breaches, in which malevolent parties could take advantage of credential theft or weakness to jeopardize the integrity and confidentiality of data kept in the cloud. Furthermore, failure to implement MFA as a basic security control to safeguard sensitive data can result in compliance violations due to a variety of regulations and security standards.

No control over the inbound and outbound network traffic.

Unauthorized users may be able to take control of servers or cloud instances if SSH access is granted without restriction. This increases the risk of data breaches, system compromises, and even lateral network movement. Moreover, it raises the possibility of brute force attacks and puts vulnerable systems at greater risk of being exploited by bad actors. To reduce these risks and strengthen security in the cloud infrastructure, SSH access must be limited to authorized users and trusted IP ranges.

Lack of Policies.

Without bucket policies, there's limited control over who can access, modify, or delete data in object storage, increasing the risk of unauthorized access and data exposure. The lack of firewall policies for network security means that there's no defined rule set to control inbound and outbound traffic, potentially leaving the cloud environment vulnerable to cyberattacks and unauthorized network access. Both policies are crucial for maintaining data integrity, securing access, and mitigating the risks of data breaches and security incidents in a cloud infrastructure.

No backup policy in place.

The business is very exposed to the effects of unforeseen disasters or system failures in the lack of a thorough backup and disaster recovery plan. The company runs a serious risk of significant data loss without a well-thought-out plan in place, which could jeopardize the accuracy of vital data and possibly cause problems with regulatory compliance. Long-term downtime can negatively affect the company's ability to recover quickly, have a severe financial impact, and erode customer trust. For these reasons, it is critical to quickly implement a strong disaster recovery and backup solution.

No snapshots of instances stored.

In the event of a successful cyberattack, the lack of "snapshots" for virtual machine instances poses a serious risk. The absence of these snapshots means that the company does not have a point-in-time backup of its virtual machines, which makes it more challenging to recover the system from an attack to its pre-attack, uncompromised state. This highlights the significance of putting in place a strong backup and recovery plan to close this crucial gap and raises the risk of data loss and system compromise in addition to impeding the organization's ability to recover quickly and maintain business continuity.

IMPACT

VPC Flow logs disabled.

Disabling VPC flow logs in a healthcare organization's cloud environment can hinder the ability to monitor and audit network traffic. This lack of visibility may make it challenging to detect and investigate security incidents, data breaches, and unauthorized access to patient data, potentially compromising data security and compliance.

Server Logging Access disabled.

When server logging access to patient data is disabled in a cloud environment, no record of who accessed the data, when, or from where is kept. Maintaining data security and compliance with patient data protection regulations may become more challenging due to this lack of visibility, which can also hinder auditing, monitoring, and investigations in the event of unauthorized access or breaches.

MFA disabled.

Patient accounts are more susceptible to illegal access without MFA, endangering the confidentiality and security of their medical records. Sensitive health information may be revealed as a result, which could violate HIPAA and other laws protecting healthcare data and have negative legal and financial repercussions.

Public security groups open to the internet.

Security risks to patient data may arise from leaving a security group (PublicSG) open to the internet and leaving port 22 (SSH) open. This setup could give unwanted users access to the system, which could result in data breaches, privacy violations, and compliance problems. These could have major repercussions for the healthcare provider's reputation and legal standing.

Instance security group open to the internet.

Security risks to patient data may arise from leaving a security group (Instance SG) open to the internet and leaving port 22 (SSH) open. This setup could give unwanted users access to the system, which could result in data breaches, privacy violations, and compliance problems. These could have major repercussions for the healthcare provider's reputation and legal standing.

Lack of bucket policy

Without a bucket policy, access control rules for patient data stored in an Amazon S3 bucket are not established, which could result in unrestricted and public access to the information. This lack of access controls puts patient data security and privacy at risk by exposing data, allowing unauthorized access, and raising the possibility of data breaches.

Lack of network firewalls.

In a healthcare setting, turning off a network firewall can lead to a serious security lapse that could expose patient data to cyberattacks and illegal access. The organization is more susceptible to network attacks, data breaches, and non-compliance with healthcare data protection regulations when its firewall is not active. This puts patient data at risk and may have negative legal and reputational effects.

No backup strategy in place

First, it exposes data and vital systems to irreversible loss in the case of hardware malfunctions, data corruption, or cyberattacks, which could cause significant data loss and system outages. Second, insufficient data backups can jeopardize disaster recovery efforts by making it more difficult for the company to promptly restore services and continue with vital operations, which in turn increases the impact of unforeseen disruptions or security incidents. Last but not least, if there are no backups, there may be problems with regulatory compliance. Since many sectors require data protection and retention, it is crucial to set up thorough cloud backup and recovery procedures.

No snapshots of instances stored.

Because there aren't easily accessible point-in-time backups to restore from, the company is left open to data loss and service interruptions in the event of system malfunctions, cyberattacks, or inadvertent deletions. Second, the inability to restore to a known, uncompromised state is seriously jeopardized in the absence of snapshots, which makes it difficult to effectively recover from security lapses or incidents. Finally, failure to meet data retention and protection requirements may compromise regulatory compliance, underscoring the vital significance of putting snapshot-based backup and recovery procedures in place on the cloud.

RECOMMENDATIONS

Enable VPC Flow Logs.

It is recommended that VPC Flow Logs be enabled for packet Rejects for VPCs. To obtain comprehensive details about the packets that are denied at a security group or NACL rule, one can enable Flow Logs. Security teams can gain valuable insights into potential threats, unauthorized access attempts, and misconfigurations within the VPC by using this information.

Enable server access logging.

Ensure that S3 buckets have Logging enabled. CloudTrail data events can be used in place of S3 bucket logging. If that is the case, this finding can be considered a false positive. Although logging S3 buckets is common, CloudTrail data events offer an additional way to monitor activity in S3 buckets. If CloudTrail sufficiently satisfies the requirement of monitoring and auditing access to the buckets, a finding of missing S3 bucket logging may be regarded as a false positive if CloudTrail data events are used for this purpose.

Enable MFA.

Enable hardware MFA device for an IAM user from the AWS Management Console; the command line; or the IAM API. IAM users can greatly improve account security and access control by implementing hardware MFA, which requires them to provide an extra layer of authentication. This is especially important when performing sensitive actions or gaining access to vital resources within the AWS environment.

Use a Zero Trust approach.

Narrow ingress traffic as much as possible. Consider north-south as well as east-west traffic. This entails closely examining and managing all incoming network traffic, including traffic coming from outside sources (north-south traffic) and traffic moving within the network (east-west traffic), to make sure that every exchange is validated and approved in accordance with stringent access controls and identity verification. In line with contemporary security best practices, this strategy reduces the attack surface, improves security, and lessens the possibility of unauthorized access or lateral movement within the network.

Encryption in transit.

Ensure that S3 buckets have encryption in transit enabled. This implies that data is shielded from interception and eavesdropping while it moves between your systems and S3 storage. In accordance with best practices for data security and privacy, you can lower the risk of data breaches and unauthorized access during transit by enabling encryption in transit, which guarantees that sensitive data is secure throughout the entire data transfer process.

Enable Network Firewall.

Ensure all VPCs have Network Firewall enabled. By enabling you to create and implement security policies for incoming and outgoing traffic filtering and inspection at the network level, Network Firewall adds another layer of defense. You can actively manage and control network traffic, reducing the risk of security threats, unauthorized access, and potential data breaches, and ultimately improving the overall security posture of your cloud environment by making sure that Network Firewall is enabled in each VPC.

Developing a backup strategy in place.

Adopt a thorough backup plan that includes frequent, automated backups of your cloud environment's infrastructure and important data. Use third-party services or cloud-native backup solutions to guarantee data availability and integrity in the event of system outages, security events, or data loss.

Proper storage of snapshots of instances.

For your cloud instances, create a strong snapshot-based backup plan to guard against system intrusions and data loss. Maintain consistent snapshots of your virtual machines so that you have solid backups in case of hardware malfunctions, cyberattacks, or unintentional data corruption.

CONCLUSION

To sum up, the evaluation of our healthcare cloud infrastructure's disaster recovery has identified both its advantages and disadvantages. We have strong privacy policies and data protection in place as evidence of our commitment to patient data security and service continuity. But the study also showed that we needed to improve our preparedness for disaster recovery by improving redundancy and failover capabilities and streamlining recovery time targets.

REFERENCES

https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/disaster-recovery-workloads-on-aws.html?did=wp_card&trk=wp_card

https://aws.amazon.com/compliance/gdpr-center/

https://docs.aws.amazon.com/

https://aws.amazon.com/compliance/hipaa-compliance/

https://aws.amazon.com/blogs/security/