Cloud Incident Response Plan

Why We Need This Plan?

The purpose of this plan is to help us know exactly what to do when something goes wrong with our cloud systems, like a security issue or an attack.

This way, we can fix things quickly, minimize any damage, and get everything back to normal as soon as possible.

Cloud Infrastructure Overview

The organization's cloud infrastructure is deployed across **two AWS regions**:

- **Multi**-Region Setup: Two **AWS** regions with Virtual Private Clouds, supporting redundancy and resilience.
- **Public** Subnets: Each VPC hosts 4 EC2 instances, resulting in 8 instances total to run the application.
- **Private** Subnets: Contains RDS (PostgreSQL) databases, configured with multi-AZ deployment for high availability.

Security Measures

- **Internet Gateway** manages external traffic.
- Security **Groups** and Network **ACLs** control inbound and outbound traffic.
- **Load Balancer – CloudFront** provide content delivery and distribute traffic across instances.
- **AWS WAF** safeguards the application against common web exploits
- **AWS Shield** mitigates Distributed Denial of Service (DDoS) attacks.

Monitoring and Logging

- **AWS CloudWatch** monitors CPU utilization, network traffic, and service health.
- **VPC Flow Logs** capture network traffic for analysis.
- **CloudTrail** tracks API calls and configuration changes.
- **AWS** Config monitors resource configurations for drift detection and compliance.

Security Controls

- **IAM** Roles – **Policies** enforce least privilege access.
- **Multi-factor** Authentication for all IAM users.
- **Encryption** at **Rest** and In-**Transit** for data stored in S3 and RDS databases.
- Automated **patching** ensures EC2 instances are regularly updated, enhancing network hardening.

Who's In Charge?

- Incident Response Team **Leader**: Makes big decisions – coordinates everyone.
- Cloud **Security Analyst**: Figure out issue – collect evidence – analyse the issue.
- Cloud **Administrator:** Makes sure the cloud systems are running well again.
- **Compliance Officer:** Ensures we handle everything according to the law.
- **Communications Officer**: Telling the right people (customers – media) what's going on, if necessary.

Incident examples:

- **Data Breach**: Unauthorized access to sensitive information.
- Denial of Service (**DoS**) Attack: Hackers overwhelm our cloud servers to slow it.
- **Account Compromise**: Someone's account gets hacked.
- **Misconfiguration**: Setting up the cloud systems incorrectly.

Incident Response Phases

1st. Preparation

- Conduct regular training for the IRT on cloud-specific threats.
- Ensure cloud systems have up-to-date monitoring and logging.
- Implement access controls and encryption to protect data.

2nd. Detection and Analysis

- **Identify** suspicious activity through cloud monitoring tools (e.g., AWS CloudTrail)
- **Verify** if the incident is genuine by cross-checking logs, alerts, and reports.
- **Analyze** the extent of the incident, affected systems, and potential data loss.

3rd. Containment

- **Short**-term **Containment**: Immediately isolate affected resources to prevent further damage (e.g., disconnect compromised VMs).
- **Long**-term **Containment**: Apply security patches, block malicious IPs, or reset passwords as needed.

4th. Eradication

- **Identify** root cause of the incident (e.g., vulnerability, malware, phishing attack).
- **Remove** all malicious artifacts (e.g., delete infected instances, remove malware).
- **Harden** the cloud environment to prevent recurrence (e.g., improve security configurations, patch vulnerabilities).

5th. Recovery

- Restore cloud services and data from backups (if required).
- Monitor systems closely to ensure normal operations are restored correctly
- Test the system to verify it's secure.

6th. Lessons Learned

- **Conduct** a post-incident review with the IRT.
- **Document** what went wrong, what went well, and areas for improvement.
- **Update** the incident response plan and security measures as needed.

Communication Plan

- **Internal** Communication: Notify relevant personnel within the organization about the incident.
- **External** Communication: Inform customers, stakeholders, and, if necessary, regulatory bodies about the breach while maintaining transparency.

Post-Incident Activities

- **Review** and **Documentation**: Complete a detailed report outlining the incident, response efforts, and future preventive measures.
- **Training** and **Updates**: Use the incident as a learning opportunity to update staff training and adjust security policies.

Cloud Environments Communication and Escalation Protocols

Communication Channels:

- **Internal**: Use platforms like Slack or Teams for real-time coordination.
- **External**: Notify clients, third-party vendors, and AWS Support as needed.
- **Incident** Reporting: Track incidents via AWS Security Hub or similar tools.

Escalation Tiers:

- **Tier 1** (**Low**-Level Incidents): Minor issues handled by on-call DevOps. Escalate if unresolved within 30 minutes.
- **Tier 2** (**Medium**-Level Incidents): Unauthorized access or performance issues. Escalate to the IRT lead or AWS Support if unresolved in 1 hour.
- **Tier 3** (**High**-Level Incidents): Major breaches or outages. Immediate response from IRT, AWS Shield, and legal team; notify executives and stakeholders.

Incident Severity:

- P1 (**Critical**): **Immediate** action, executives notified within 15 minutes.
- P2 (**High**): Action within **30 minutes**, escalate in 1 hour.
- P3 (**Medium**): Action within **1 hour**, escalate in 4 hours.
- P4 (**Low**): Resolved within **24 hours**, escalate if persistent.

Post-Incident Communication:

- Prepare reports
- Hold review meetings
- Notify clients