Cloud Computing Security & Management

Assignment-3

Name - Amartya Kumar
Sap Id - 500097356
Batch - B4

Assignment-3

Question 1: Identity and Access Management.
You are working as a Cloud Security Analyst for a mid-sized company that recently migrated its infrastructure to Google Cloud. The organization is concerned about unauthorized access to its cloud resources. Your manager asks you to implement the best practices of Identity and Access Management (IAM) to secure the cloud environment.

➔ What is IAM in the context of cloud security?

Ans:- In cloud security, Identity and Access Management (IAM) refers to the set of rules and tools that guarantee the proper people and services have access to cloud resources while blocking unwanted access. IAM gives administrators fine-grained access control in Google Cloud, enabling them to decide who may do what on which resources.

Important elements of Google Cloud's IAM include:
Identities: These are people who require access to cloud resources, such as Google Groups, service accounts, and accounts.
Roles: Groups of permissions that specify what can be done with resources.
Policies: Relationships between roles and identities that define who can access what resources.
Resources: The cloud assets that are being safeguarded, such as databases, storage, virtual machines, projects, etc.
Because it creates the authorization framework that governs access to all other security measures and cloud resources, IAM is essential to cloud security because it serves as the first line of defense against unwanted access.

➔ How would you implement the principle of least privilege for users and service accounts?

Ans:- Here's how to implement the principle of least privilege in Google Cloud:
For Users: Implement time-bound access through temporary role assignments for special projects; Regularly review and revoke unnecessary permissions through access reviews, define job-specific roles based on responsibilities rather than assigning broad predefined roles; Use custom roles to provide precisely

tailored access permissions; and Think about Just-In-Time access for sensitive operations rather than permanent access.

About Service Accounts:
For particular apps or features, create specialized service accounts.
Allocate each service account simply the bare minimum of necessary permissions.
Limit the development of service account keys and use frequent key rotation.
Utilize OAuth and workload identity federation to use temporary credentials whenever feasible.
Instead of exchanging keys for administration tasks, set up service account impersonation.
Use resource-level limitations to restrict the range of activities that a service account can perform.

➔ What types of IAM roles would you assign to different team members (e.g., Developer, Admin, Security Analyst)?

Ans:- Regarding Developers:
Roles/compute.viewer (to view compute resources) is the role to assign.
To execute builds, use roles/cloudbuild.builds.builder.
positions/logging.viewer (for log viewing) (For suitable buckets) roles/storage.
objectViewer
Personalized roles with particular development resource permissions
Limitations:
No direct access to production
No authorization to change IAM policies
Project-wide roles as opposed to resource-specific access.

To the Administrators:
roles/compute is the role to assign. Admin (oversaw storage and computing resources) roles. admin roles/monitoring.admin (for system monitoring) roles/logging (for storage management). administrator (for log management)
Implementation Remarks:
accounts that are distinct for privileged and ordinary operations
Break-glass protocols should be used for emergency entry.
Put permission procedures in place for sensitive modifications.

For those who work as security analysts:
roles/logging.viewer (full log access) is the role to assign.
Security operations: roles/securitycenter.admin

/iam.security roles Examiner (to examine but not change policies)
roles/monitoring.viewer (to keep track of alerts and performance)

➔ How would you monitor and audit IAM policies for compliance?

Ans:- Implementing IAM best practices can significantly reduce the risk of unauthorized access and maintain operational efficiency in Google Cloud. These practices include real-time monitoring through Cloud Audit Logs, regular auditing using IAM Recommender and Policy Analyzer, and compliance reporting by mapping IAM controls to specific requirements like SOC 2, HIPAA, and PCI-DSS. Documenting policy exceptions and maintaining an audit trail of policy changes with justifications is also essential.
Governance involves defining a clear policy ownership and responsibility matrix, establishing formal procedures for granting temporary elevated privileges, implementing mandatory access reviews, and creating processes for revoking access upon role changes or terminations.
Comprehensive IAM documentation and training programs are also essential. By implementing these best practices, organizations can significantly reduce the risk of unauthorized access while maintaining operational efficiency in Google Cloud.

Question 2: Data Protection in Cloud Storage
Your team is developing a healthcare application on Google Cloud Platform that stores sensitive patient data in Cloud Storage buckets. As the Cloud Security Engineer, you are responsible for ensuring that the data is protected from unauthorized access and breaches.

➔ Methods to secure data at rest and in transit in GCP

Ans:- 1. Protecting Data While It's in Transit and at Rest
Default Encryption: Make use of Google Cloud Storage's server-side encryption, which is automatically applied to all saved data.
Increased control over encryption keys can be achieved by implementing customer-managed encryption keys, or CMEK.
Object Versioning: Turn on versioning to help with recovery and avoid unintentional deletions.
Retention Policies: Establish minimal retention durations to avoid erasing data too soon.
Protection of Data in Transit

Enforce TLS: All API contacts with Cloud Storage must use TLS 1.2+.
Only Use HTTPS: Use bucket policies to set up buckets to refuse non-HTTPS connections.
VPC Service Controls: Put these controls in place to limit data flow beyond specified security boundaries.
Private Google Access: To reduce exposure to the public internet, set up private endpoints for services when appropriate.

➔ How to use encryption keys (Google-managed vs. Customer-managed)

Ans:- 2. Key Management for Encryption
Keys Managed by Google (Default)
Automatic Protection: Google-managed AES-256 encryption keys automatically encrypt all data.
Zero Configuration: No setup or administrative effort is necessary.
Key Rotation: Google manages key rotation and rotation automatically.
Limitation: Limited access and audit visibility into critical operations
Encryption keys managed by the customer (CMEK)
Execution: Use Cloud Key Management Service (KMS) to generate and manage keys.
Enhanced Control: Retain possession of the encryption keys that safeguard your information.
Schedule for Key Rotation: Rotate your keys every quarter.
Revocation Ability: The ability to disable or destroy encryption keys to revoke access
Audit Trail: Keep thorough records of all important management and usage operations.
It is highly advised that CMEK be used for sensitive medical data.

➔ How to control access to Cloud Storage buckets (ACLs vs. IAM policies)

Ans:- Cloud Storage Access Control for Identity and Access Management (IAM) Policies
Main Control Technique: Make IAM your main access control system.

Access Based on Roles: Use both preset and custom roles to apply the principle of least privilege.
Hierarchy of Resources: Apply permissions at the bucket, project, folder, and organization levels.

Accounts for Services: For application access, use dedicated service accounts with restricted rights.
Conditional Entry: Put in place context-aware access controls according to the location, status, and other factors of the device.
Lists of Access Control (ACLs)
Restricted Use: Use IAM policies instead of ACLs as much as possible. Use legacy support only when it's necessary for interoperability with other systems. Turn on Uniform Bucket-Level Access to use IAM alone to enforce consistent access control.

➔ Any additional best practices for securing sensitive healthcare data in the cloud

Ans:- Measures for Compliance
HIPAA Compliance: Verify that all controls meet HIPAA regulations.
BAA: Complete the Google Cloud Business Associate Agreement
Frequent Audits: Perform security audits every three months under compliance requirements.
Observation and Reaction to Incidents
Turn on thorough logging for all storage access and operations using cloud audit logs.
notifications: Set up notifications for questionable activity (such as mass deletions or odd access patterns).Prevention of Data Loss (DLP): Use Cloud DLP to safeguard and scan private data.
Controls in Administration
Separation of Duties: Make sure that no employee has complete access to every part.
Frequent Access Reviews: Verify permissions by conducting access reviews every three months.
Enforcement of Security Keys: Hardware security keys must be used to gain administrative access.
Management of Data
Data categorization: Assign each stored object a tag and a categorization.
Data Lifecycle: Clearly define guidelines for safe deletion and data retention.
De-identification: Where applicable, use the Cloud Healthcare API to de-identify PHI.
When correctly applied, this tactic offers a thorough method for protecting private medical information stored in Google Cloud Storage while adhering to all applicable laws.