**IS ASSIGNMENT # 2**

**HASSAN ALI**

**K20-1052 BSE-7B**

**Seven Cloud Security Risks with Real-World Examples**

1. **Abuse and nefarious use of cloud computing**: A criminal group uses compute instances from Azure/AWS (free trial) and installs mining software to mine cryptocurrency. They are able to mine substantial sums over several months before the cloud provider detects the unusual activity and shuts the instances down.

2. **Insecure interfaces and APIs**: A mobile app connects to a cloud-based database (Firebase) to store user data. The app uses plain HTTP requests instead of encrypted HTTPS, allowing an attacker on the same public WiFi network to intercept credentials and gain access to the database.

3. **Malicious insiders**: A systems administrator at a cloud hosting company is fired. As revenge, before leaving the company he misconfigures firewall policies and disables log collection for customer instances that he had access to. This results in a breach of sensitive customer data.

4. **Shared technology issues**: A public cloud provider uses a shared virtualization hypervisor (like Azure does that is known as multi-tenancy) to isolate customer VMs. A zero-day exploit in the hypervisor allows one customer's VM to break out and access virtual disks belonging to other customers on the same physical server.

5. **Data loss or leakage**: A cloud customer misconfigures access controls on an object storage bucket (can be Azure Storage Blob). The bucket is indexed by search engines and accessible to anyone online. An attacker finds sensitive customer data exposed in the bucket via a Google search.

6. **Account or service hijacking**: The password for a cloud services admin account is compromised through a phishing attack. Since there was no two factor authentication, the attacker uses the password to log into the account, changes the email and resets passwords for other admin accounts. The attacker now has full control of the customer's cloud services and data.

1. **Insecure or incomplete data deletion**: A cloud customer deletes data (deleting a VM on Azure) but the cloud provider only removes pointers to the data instead of overwriting it. The customer's supposedly deleted data is later recovered by another customer who is assigned the same physical storage.

**Here are more detailed explanations and countermeasures for each cloud security risk:**

1. Abuse of cloud computing resources:

- How it happens: Attacker rents cloud instances and uses them for crypto mining, DDoS, spam, etc. Hard to detect as it looks like normal customer workload.

- Countermeasures: Cloud provider implements better analytics to detect unusual usage patterns. Customers monitor usage closely and set alerts. Use of 2FA and IP allowlisting helps prevent unauthorized instance access.

2. Insecure interfaces and APIs:

- How it happens: App uses insecure HTTP instead of HTTPS to access cloud APIs and resources. Traffic is exposed to MITM attacks.

- Countermeasures: Enforce use of latest TLS version for all cloud APIs and interfaces. Proper certificate validation and TLS cipher configuration. API access restricted to authorized sources.

3. Malicious insider:

- How it happens: Rogue employee with privileged access misuses it for revenge or gain before leaving company.

- Countermeasures: Access monitoring, principle of least privilege. Timely deprovisioning of access for departing employees. Logs monitored to detect unauthorized activity.

4. Shared technology exploit:

- How it happens: Hypervisor vulnerability allows VMs to access each other's data.

- Countermeasures: Prompt hypervisor patching, hardware-assisted virtualization, isolate customers on separate physical servers.

5. Data leakage:

- How it happens: Misconfigured cloud storage allows public access to private data.

- Countermeasures: Access controls and 'private by default' configurations. Auditing and remediation of misconfigurations. Data loss prevention controls.

6. Account hijacking:

- How it happens: Attacker gains access to cloud control plane through compromised credentials.

- Countermeasures: MFA, password managers, audit account activity. Access controls and privileged access management.

7. Incomplete data deletion:

- How it happens: Deleted data not completely overwritten. Later recovered by another customer.

- Countermeasures: Use provider with guaranteed wipe and overwriting. Encrypt data prior to upload.