**Incident Overview:**

* **Company Name:** KZM Retail
* **Date:** October 2024
* **Type of Incident:** Data Breach
* **Scope:** Unauthorized access to sensitive customer information (credit card data and personal details) across applications, networks, systems, and data repositories.
* **Affected Resources:** Virtual machines, Cloud Storage buckets, Firewalls.

**Details of the Incident:**

The security team detected unusual activity within the company’s infrastructure. Upon further investigation, it was revealed that attackers had gained unauthorized access to customer data. The breach involved compromised virtual machines with public IP addresses, misconfigured firewall rules allowing unrestricted access, and publicly accessible storage buckets containing sensitive information.

**Vulnerabilities Identified:**

1. **Compute Engine VM (cc-app-01):**
   * Public IP address
   * Secure Boot disabled
   * Use of default service account with full API access
   * Malware: bad domain activity detected
2. **Cloud Storage Bucket:**
   * Public bucket ACL allowing anonymous access
   * Bucket policy disabled, leading to unrestricted access
   * Bucket logging disabled
3. **Firewall:**
   * Open SSH (TCP port 22) and RDP (TCP port 3389) to the entire internet
   * Firewall rule logging disabled

**Remediation Actions Taken:**

1. **Shutting Down and Replacing Compromised VM (cc-app-01):**
   * Shut down the infected VM to halt malicious activity.
   * Created a new VM (cc-app-02) from a clean snapshot with enhanced security (disabled public IP, Secure Boot enabled, no full API access).
   * Deleted the compromised VM to eliminate further risk.
2. **Securing Cloud Storage Buckets:**
   * Revoked public access and removed all user permissions.
   * Switched to uniform bucket-level access control to prevent unauthorized data access.
3. **Restricting Firewall Access:**
   * Created new firewall rules to restrict SSH access only to authorized IP ranges.
   * Deleted overly permissive firewall rules (open ICMP, SSH, and RDP).
   * Enabled logging on the remaining firewall rules to monitor traffic.

**Compliance Verification:**

After remediating the vulnerabilities, I re-ran the PCI DSS 3.2.1 compliance report to confirm the environment now met industry security standards. All high and medium severity vulnerabilities were successfully mitigated.

**Conclusion:**

The breach was contained, the compromised systems were remediated, and the company’s security posture was restored. This incident reinforced the importance of maintaining strict security controls, monitoring network traffic, and ensuring compliance with regulatory standards to prevent future breaches.