### **Discussion Questions for the Capital One Data Breach (2019)**

Answer the following questions based on the information provided about the Capital One data breach. You are encouraged to use diagrams and charts to illustrate your ideas.

**1. What happened in the Capital One data breach of 2019?**

* A) A former employee hacked into Capital One's mobile banking app and stole customer data.
* B) A hacker exploited a misconfiguration in Capital One’s cloud infrastructure, allowing unauthorized access to sensitive data of over 100 million customers.
* C) Capital One's internal systems were compromised by ransomware.
* D) An employee accidentally leaked customer data through unsecured email.

**Answer: B) A hacker exploited a misconfiguration in Capital One’s cloud infrastructure, allowing unauthorized access to sensitive data of over 100 million customers.**

**2. What are two effective security mechanisms to guard against vulnerabilities in cloud environments?**

* A) Implementing proper Identity and Access Management (IAM) policies and conducting regular cloud configuration audits.
* B) Disabling all cloud services and moving to on-premise servers.
* C) Using weak encryption to save processing time.
* D) Allowing all employees full access to cloud services for efficiency.

**Answer: A) Implementing proper Identity and Access Management (IAM) policies and conducting regular cloud configuration audits.**

**3. If you were a hacker, how would you realistically launch a similar attack on another financial institution using cloud services?**

* A) Perform reconnaissance to identify cloud misconfigurations, use social engineering to obtain cloud credentials, and exploit overly permissive IAM policies to access sensitive data.
* B) Hack into the financial institution’s website and download data directly from the homepage.
* C) Use a brute-force attack to guess passwords.
* D) Send phishing emails to all customers.

**Answer: A) Perform reconnaissance to identify cloud misconfigurations, use social engineering to obtain cloud credentials, and exploit overly permissive IAM policies to access sensitive data.**

**4. How can companies mitigate the risk of insider attacks in cloud-based environments?**

* A) Implement role-based access control (RBAC), use activity monitoring tools, and enforce the principle of least privilege for all users.
* B) Allow all employees full access to cloud services at all times.
* C) Encourage employees to use the same password across multiple platforms.
* D) Disable all logging to reduce storage costs.

**Answer: A) Implement role-based access control (RBAC), use activity monitoring tools, and enforce the principle of least privilege for all users.**

**5. How can vulnerability scanning be conducted in cloud infrastructure?**

* A) Use tools like AWS Inspector, Qualys, or Nessus to detect misconfigurations, unpatched software, and weak access controls.
* B) Manually check each server for vulnerabilities.
* C) Disable all cloud security measures temporarily to scan for weaknesses.
* D) Only scan the development environment to save resources.

**Answer: A) Use tools like AWS Inspector, Qualys, or Nessus to detect misconfigurations, unpatched software, and weak access controls.**

**6. As the CTO of Capital One, what measures would you implement to enhance cloud security while maintaining operational efficiency?**

* A) Use encryption for all data at rest and in transit and implement automated security monitoring with alerts for suspicious activity.
* B) Disable encryption to speed up data access.
* C) Require all employees to work from the same physical office.
* D) Allow public access to all cloud resources for testing purposes.

**Answer: A) Use encryption for all data at rest and in transit and implement automated security monitoring with alerts for suspicious activity.**

**7. How should companies balance the need for strong firewall protections with the flexibility required in cloud environments?**

* A) Use dynamic firewall rules that automatically adjust based on traffic patterns and implement strict access control lists (ACLs) for sensitive data.
* B) Disable all firewalls to avoid disruptions.
* C) Only use firewalls for external traffic but ignore internal traffic.
* D) Set firewalls to block all traffic, regardless of source.

**Answer: A) Use dynamic firewall rules that automatically adjust based on traffic patterns and implement strict access control lists (ACLs) for sensitive data.**

**8. How can companies improve monitoring and response times to detect breaches like the Capital One attack?**

* A) Implement real-time monitoring with Security Information and Event Management (SIEM) tools and establish incident response protocols to quickly address breaches.
* B) Only check for breaches during business hours.
* C) Disable monitoring to avoid alert fatigue.
* D) Wait for customers to report suspicious activity.

**Answer: A) Implement real-time monitoring with Security Information and Event Management (SIEM) tools and establish incident response protocols to quickly address breaches.**

**9. What weaknesses were present in Capital One’s cloud security practices that led to the breach?**

* A) Misconfigured firewall settings, weak IAM policies, and insufficient monitoring of cloud activity.
* B) Lack of antivirus software in the cloud.
* C) No backups of customer data.
* D) Use of unencrypted data for internal testing.

**Answer: A) Misconfigured firewall settings, weak IAM policies, and insufficient monitoring of cloud activity.**

**10. As the CIO of Capital One, how would you improve cloud security and protect sensitive data?**

* A) Implement stronger IAM policies, enforce regular cloud security audits, and use encryption for all sensitive data.
* B) Disable cloud access for all employees.
* C) Store customer data in plaintext to reduce complexity.
* D) Remove all security measures for faster access to data.

**Answer: A) Implement stronger IAM policies, enforce regular cloud security audits, and use encryption for all sensitive data.**

4o