### **Discussion Questions for the Deloitte and Accenture Data Breaches (2017)**

Answer the following questions based on the information provided about the Deloitte and Accenture data breaches. You are encouraged to use diagrams and charts to illustrate your ideas.

**1. What happened in the Deloitte data breach of 2017?**

* A) Hackers exploited a misconfiguration in Deloitte's cloud storage to access client emails and sensitive data.
* B) A phishing attack allowed hackers to steal customer credit card information from Deloitte's website.
* C) An internal server at Deloitte was compromised, exposing user passwords.
* D) Deloitte’s internal app was hacked, leaking confidential project details.

**Answer: A) Hackers exploited a misconfiguration in Deloitte's cloud storage to access client emails and sensitive data.**

**2. What are two effective security mechanisms to prevent similar breaches in large organizations like Deloitte?**

* A) Implementing multi-factor authentication (MFA) and encrypting sensitive data in transit and at rest.
* B) Allowing all employees to have full access to internal systems.
* C) Disabling internal firewalls to simplify workflows.
* D) Using weak encryption methods to reduce overhead.

**Answer: A) Implementing multi-factor authentication (MFA) and encrypting sensitive data in transit and at rest.**

**3. As a security consultant for Deloitte, how would you advise the company to improve its internal security protocols?**

* A) Implement strict access control policies, enforce regular security training for employees, and use encryption for all sensitive communications.
* B) Use the same passwords for all internal applications.
* C) Only allow encryption for financial transactions.
* D) Stop monitoring internal traffic to increase performance.

**Answer: A) Implement strict access control policies, enforce regular security training for employees, and use encryption for all sensitive communications.**

**4. How can organizations improve cloud storage security to prevent data leaks?**

* A) Use proper access controls, enable encryption, implement logging and monitoring, and ensure cloud configurations are regularly reviewed and patched.
* B) Allow public access to all cloud storage for convenience.
* C) Disable encryption to improve access speed.
* D) Only use cloud storage for temporary files.

**Answer: A) Use proper access controls, enable encryption, implement logging and monitoring, and ensure cloud configurations are regularly reviewed and patched.**

**5. How can effective cloud security audits be conducted?**

* A) Use tools like AWS Trusted Advisor, Azure Security Center, and manual reviews to detect misconfigurations and vulnerabilities in cloud environments.
* B) Only audit internal servers, as cloud platforms are inherently secure.
* C) Perform audits only once a year to reduce costs.
* D) Rely solely on cloud service providers to handle security without internal oversight.

**Answer: A) Use tools like AWS Trusted Advisor, Azure Security Center, and manual reviews to detect misconfigurations and vulnerabilities in cloud environments.**

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

* A) Automate security updates, enable encryption for all cloud services, and deploy cloud-specific monitoring tools to detect unauthorized access.
* B) Disable monitoring to reduce cloud service costs.
* C) Limit security patches to avoid disruptions during business hours.
* D) Allow full public access to all cloud services for testing purposes.

**Answer: A) Automate security updates, enable encryption for all cloud services, and deploy cloud-specific monitoring tools to detect unauthorized access.**

**7. How can companies balance the need for rapid deployment with the necessity of thorough security checks?**

* A) Implement DevSecOps practices to integrate security checks into every stage of the development and deployment process.
* B) Deploy updates without any security checks to avoid delays.
* C) Only run security checks after deployment.
* D) Delay updates until security checks can be completed, even if it takes months.

**Answer: A) Implement DevSecOps practices to integrate security checks into every stage of the development and deployment process.**

**8. What steps would you take to improve vulnerability management practices and prevent incidents like the Deloitte and Accenture breaches?**

* A) Regularly patch systems, implement automated vulnerability scanning, and prioritize fixing critical vulnerabilities identified by tools like Nessus or Qualys.
* B) Only patch vulnerabilities when there is a known attack.
* C) Allow outdated systems to continue running to avoid disruption.
* D) Rely solely on firewalls to prevent vulnerabilities from being exploited.

**Answer: A) Regularly patch systems, implement automated vulnerability scanning, and prioritize fixing critical vulnerabilities identified by tools like Nessus or Qualys.**

**9. What IT weaknesses were present in Deloitte’s and Accenture’s systems that enabled the breaches?**

* A) Lack of multi-factor authentication, weak access controls, and poorly configured cloud storage.
* B) Use of outdated encryption methods and unmonitored cloud infrastructure.
* C) Too many firewalls blocking internal communication.
* D) Relying on external vendors for all security matters.

**Answer: A) Lack of multi-factor authentication, weak access controls, and poorly configured cloud storage.**

**10. As the CIO of Deloitte or Accenture, how would you improve IT security and protect sensitive client data?**

* A) Implement comprehensive data encryption, enforce strict access control policies, conduct regular security audits, and implement multi-factor authentication for all sensitive systems.
* B) Only patch systems once a year to reduce costs.
* C) Limit the use of encryption to save processing power.
* D) Reduce monitoring of internal systems to improve speed.

**Answer: A) Implement comprehensive data encryption, enforce strict access control policies, conduct regular security audits, and implement multi-factor authentication for all sensitive systems.**