Lab - Recommend a Cloud Security Solution

Solis, Rein Aldwin E.

33 - ITE - 01

Objectives

Part 1: Research and Recommend a Cloud Model and a Cloud Service Model

Part 2: Identify Shared Responsibility for Cloud Services and Cloud Security

Part 3: Identify Five Security Threats Related to Cloud Computing

Part 4: Identify Five Security Measures for Deploying eCommerce in Cloud

Background / Scenario

In this research-oriented lab, you will research information about cloud computing security and prepare for a recommendation for an organization that is deploying their eCommerce option to the cloud.

A startup company is considering a cloud solution for their eCommerce business. The company designs and sells customized clothing and home decoration items to customers around the world. The company hopes the cloud solution can provide key functions including:

- Product search and display with multiple presentations (searching, zooming, and viewing from different angles, etc.)
- Product ordering (order confirmation, delivery tracking and notification, order history, etc.)
- Customer service
- Advertising and promotion
- Sales tracking and reporting

As an IT security specialist, you are asked to research and prepare a report evaluating potential cloud solutions and their security implications.

Required Resources

- A computer with internet access

Instructions

Part 1: Research and Recommend a Cloud Model and a Cloud Service Model

Cloud models include public cloud, private cloud, hybrid cloud, and community cloud. Cloud service models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Which cloud service model would you recommend to meet the feature requirements of the company? Explain.

Platform as a Service (PaaS) is what I advise. For a new eCommerce business, PaaS offers the ideal ratio of convenience and control. Because the cloud provider manages the underlying infrastructure, developers can focus on creating and implementing apps. This facilitates the quick creation and implementation of order processing, customer assistance apps, product displays, and other features.

Part 2: Identify Shared Responsibility for Cloud Services and Cloud Security

Think about shared responsibility for security between the company and a cloud provider for the cloud service model recommended. Use the table below and mark each box with Client, Shared, or Cloud Provider.

Record your chosen cloud service model:

Enter the security responsibilities for your chosen cloud service model:

Description	Cloud Service Security Responsibility
Data	**Client**
Endpoints	**Shared**
Identity Management	**Shared**
Application	**Cloud Provider**
Network Control	**Cloud Provider**
Operating System	**Cloud Provider**
Physical Infrastructure	**Cloud Provider**

Description	Cloud Service Security Responsibility
Data	Client
Endpoints	Shared
Identity Management	Shared
Application	Cloud provider
Network Control	Cloud provider
Operating System	Cloud provider
Physical Infrastructure	Cloud provider

Part 3: Identify Five Security Threats Related to Cloud Computing

List at least 5 security threats related to cloud computing.

Threat	Description
Threat 1	**Data Breaches** - Unauthorized access to sensitive customer and company data.
Threat 2	**Account Hijacking** - Attackers gaining access to employee or customer cloud accounts.
Threat 3	**Denial of Service (DoS) Attacks** - Making cloud services unavailable to legitimate users.
Threat 4	**Insecure APIs** - Vulnerabilities in the application interfaces used to interact with the cloud.
Threat 5	**Insider Threats** - Employees or contractors misusing their access to data or services.

Threat	Description
Threat 1	Blank
Threat 2	Blank
Threat 3	Blank
Threat 4	Blank
Threat 5	Blank

Part 4: Identify Five Security Measures for Deploying eCommerce Cloud Solution

Perform an internet search to find out security measures required to secure an eCommerce cloud solution.

- **Least Privilege & MFA (Multi-Factor Authentication)**: Grant users and applications only the access they need, and require multi-factor authentication for all admin and sensitive accounts.
- **Data Encryption (In-Transit and At-Rest)**: Encrypt all data during transmission and while stored using strong protocols and provider encryption tools.
- **Web Application Firewall (WAF)**: Use a WAF to block malicious web traffic and protect against threats like SQL injection and XSS.
- **Security Audits & Testing**: Regularly scan for vulnerabilities and conduct penetration tests to identify and fix security gaps.
- **Logging, Monitoring & Incident Response**: Enable centralized logging and monitoring, and maintain a tested incident response plan for quick threat mitigation.

Reflection Questions

1. What are some benefits of deploying online services in cloud?

Unmatched scalability and elasticity are two benefits of deploying online services in the cloud. This enables companies to rapidly scale up or down resources in response to demand, which is perfect for eCommerce traffic fluctuations. By using a pay-as-you-go model, it also offers great cost-effectiveness by eliminating the need for significant upfront capital expenditures on infrastructure and technology. Additionally, cloud systems provide disaster recovery capabilities,

high availability, and expanded global reach, guaranteeing that services are continuously available to clients around the globe with integrated redundancy and resilience against outages.

2. Can the company rely on the cloud solution provider for everything including services and security? Explain.

No, especially when it comes to security, the business cannot depend entirely on the cloud solution provider. The Shared Responsibility Model, a key idea in cloud computing, clarifies this misperception. Although cloud providers are in charge of the "security of the cloud" (i.e., protecting the underlying infrastructure such as physical facilities, networking, virtualization, and host operating systems), the client is still in charge of the "security in the cloud." This includes protecting their own data, cloud-deployed applications, cloud service configurations, identity and access management (i.e., who can access what), and client-side devices, irrespective of the service model (IaaS, PaaS, or SaaS). Cloud security breaches are frequently caused by people who don't comprehend and carry out their share of this obligation.