Intro to Cloud Security

Show Split View | Cloud Details | Awards | Help

Learn fundamental concepts regarding securing a cloud environment.

Chart | Scoreboard | Discuss | Writeups | More

Difficulty: Easy

Active Machine Information

Loading... *Loading...* *Loading...* *Loading...*

39%

Task 1 Introduction

Task 2 Architectural Concepts of Cloud

Task 3 Cloud Security Concepts

Task 4 Cloud Security Risks Concerning Deployment Models

This task will briefly discuss various cloud deployment models and their associated risks. Read along the following topics to get an understanding of various cloud models.

Click to enlarge the image.

Private Cloud

As studied, a private cloud is an environment in which resources are dedicated to a single customer. These are suitable for customers that are more concerned about the security of their data. Associated risks are as under:

- **Personnel threats**: This includes both unintentional and intentional threats. Customers have no control over the provider's data centre and administrators. Any insider can cause damage to customers' data (either intentionally or unintentionally).
- **Natural disasters**: Private cloud is vulnerable to natural disasters.
- **External attacks**: Multiple attacks, such as unauthorised access, Man-in-the-middle attacks, and Distributed Denial of Service, can compromise the user's data.

Public Cloud

In the public cloud, resources among users are shared with the help of virtualisation technology. Some risks include:

- **Vendor Lock-In**: The customer becomes a dependent service provider in the public Cloud. It becomes nearly impossible for the customer to move the data out of the cloud infra before the end of the contract term; thereby, the customer becomes the hostage of the provider.
- **Threat of new entrants**: Your cloud provider may provide services to your competitor in the public cloud.
- **Escalation of Privilege Authorised**: In the public cloud, users may try to acquire unauthorized permissions. A user who gains illicit administrative access may be able to gain control of devices that process other customers' data.

Community Cloud

Computing & storage infrastructure is shared between a specific community or organisation members. Some risks include:

- **Vulnerability**: In a community cloud, any node may have vulnerabilities, which can also cause intrusions on the other nodes. Also, in a community, cloud configuration management and baselines are almost impossible (and very difficult to enforce).
- **Policy and administration**: It is challenging to enforce decisions and procedures in the community cloud, posing a severe challenge and threat.

Answer the questions below

In which cloud model does the customer become the hostage of cloud providers (vendor locked in)?

public Correct Answer

Is it challenging to enforce specific business decisions and procedures in the community cloud (yea/nay)?