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...*

22%

Task 1 Introduction

Task 2 Architectural Concepts of Cloud

Task 3 Cloud Security Concepts

View Site

To understand cloud security concepts, first, we need to know what we need to protect in the cloud. The simple answer is "**Data**". Data is an asset and can be anything and any piece of information that any customer or organisation has. Data must be categorised into different levels (as defined below) before sharing in cloud platforms so that appropriate controls can be applied to protect it from a security point of view. There are three main classes of data depending on their sensitivity:

- **Confidential data:** Confidential data can be considered the most critical data any organisation can have. Confidential information/data, if exposed, can damage an organisation's reputation and even includes personally identifiable information.
- **Internal data:** Internal data is information that, if exposed, causes moderate risk or harm to the company.
- **Public data:** Public data is any information included on (or intended for) the public. There is no consequence if public data is leaked because it's already meant for use by everyone.

Cloud Data Lifecycle

In today's world, organisations store and use large amounts of data, including critical and sensitive data of the customers. Data on the cloud should be managed through its lifecycle to ensure its secure usage in every phase.

Major Steps

Data life cycle means the sequence of steps a particular data goes through from its creation to its deletion phase.

Security Aspects in Cloud Data Lifecycle

Each phase of the cloud data lifecycle requires protection. Below are the cloud data lifecycle stages, security considerations and requirements.

Create/Update

The create phase is the initial phase of the data lifecycle. It includes the newly created data and data that is being freshly imported from other data sources. In this phase, the data owner should be defined, and categorisation or classification of data should be done. Security aspects and challenges in this phase are as below:

- **Implementing SSL/TLS:** Secure communication through SSL/TLS should be implemented so that it will be difficult for the attacker to listen to data transferred between the customer and the cloud provider.
- **Encryption:** Data should be encrypted so that if data is exposed, the attacker cannot read it without decrypting it.
- **Secure connections:** Secure connections and paths should be established for the data transfer so that change of data breach is minimised (ensures data security in transit).

Store

Data is processed based on its form (structured or unstructured) and stored in a container generally known as a database. Security aspects at this stage are as below:

- **Encryption:** Data should be encrypted to protect data at rest.
- **Backup:** Backup should be taken to prevent data loss; if data is lost, it can be restored from the available backups.

Use

As we know, if data is encrypted, it must be decrypted to be used by the application. Security aspects include the following means:

- **Secure connections:** Encrypted paths should be established before data transfer to ensure the confidentiality and integrity of data in transit.
- **Secure platform:** A secure authentication mechanism should be used, protected from attacks and vulnerabilities.
- **Restrict Permissions:** Data owners should set strict permissions to modify and process data from unauthorised persons.

- **Secure Virtualisation:** There is the concept of virtualisation in cloud computing in which resources among users are shared. So cloud providers need to ensure that one customer's data should not visible to other customers.

Share
Share data within or outside the cloud infra; challenges include:
- **Jurisdiction:** Regulatory mandates/restrictions of sharing data across specific locations/regions.
- **Data Loss Prevention (DLP):** Data Loss Prevention (DLP) helps to detect and prevent data breaches or unwanted destruction of sensitive data. It contains sensitive data from being shared with unauthorised persons.

Archive
Long-term storage of data and applications; security aspects include:
- **Encryption:** Data should be encrypted before storing in cloud premises
- **Physical Security:** It demands that the storage servers are physically secured and prevented from unauthorised access through biometrics, CCTV, etc.
- **Location:** Reflects a physical location where data will be stored. Environmental factors such as natural disasters, climate, etc., can pose risks and consider Jurisdictional aspects (local and national laws) are key factors at this stage.
- **Backup Procedure:** How will data be recovered when required and How often full/incremental backups will be carried out?

Destroy
Data should be destroyed once of no use so that it cannot be misused by any user (intentional or unintentional). Crypto shredding is a process in which encrypted data is useless by destroying cryptographic keys (without keys, data cannot be decrypted).

Security Issues in the Cloud & its Solution

Despite the benefits of cloud computing, several security challenges must be addressed effectively. These challenges raise concerns about fundamental security properties such as confidentiality, integrity and availability. Significant issues are as defined below:
- **Data confidentiality:** When the data is hosted in the cloud, its privacy is at risk. As users have no physical access to their data once it has been outsourced, they don't know how the confidentiality of their data is being maintained. Cloud service providers can examine the data of the users without detection.
- **Virtualisation issues:** It allows the resources to be shared among the users. We need a mechanism to ensure isolation and secure communication between VMs. Users are not isolated in a multitenant environment, so one user can examine the data of another user.
- **Insecure interfaces and API:** Cloud services are managed by the customers with the help of software or APIs. So vulnerable software or API can be risky, and data or customer confidentiality and integrity are at risk.
- **Malicious insiders:** Some malicious insiders can cause the data breach of other clients. Taking advantage of shared technology vulnerabilities, these insiders can leak the data of other users or exploit security weaknesses, thus causing security threats to the other customers on the cloud.
- **Account or service hijacking:** Several methods can cause account or service hijacking. These include phishing frauds, vulnerability exploitation and password reuse among users.
- **Access Control Mechanism (ACM):** In a cloud computing environment, users and cloud servers are not in the same domain. Enforcing efficient and reliable access to information is critical when data is outsourced to the cloud. An unauthorised person can gain access to the data due to a lack of access control rights.

Answer the questions below

What is the first phase in the cloud data lifecycle?

create

Correct Answer

Click the **View Site** button at the top of the task to launch the static site in split view. What is the flag after completing the exercise?

Answer format: ***{**********}

Submit

Task 4 ○ Cloud Security Risks Concerning Deployment Models

Task 5 ○ Security Through Access Management

Task 6 ○ Security Through Policies

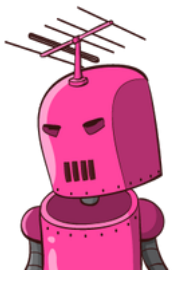
Task 7 ○ Security Through Network Management

Task 8 ○ Security Through Storage Management

Task 9 ○ Cloud Security - Some Additional Concepts

Task 10 ○ Conclusion

Created by 

tryhackme and  1337rce