- FCAIT, GLS UNIVERSITY.
- IMSc(IT)-Sem-7
- Topic Name : Cloud Security
- Cloud Computing
- 05/09/2020
- Pranjal Bhimani (04) , Chetan Dasondi (70)
- Guided By: Prof. Dinesh Kalal

Index

- What is Cloud Security and Why ?
- Public, Private , Community or Hybrid ?
- Cloud Security Precautions.
- Measures & Controls in Cloud Security.
- Cloud Security in AWS.

Why Cloud Security ?

Why cloud security important let's see:

Linkedin

In 2012 6.5 M Usernames and Passwords were hacked from linkedin databases and published to public sites.

Sony

In 2014 Sony experienced the most aggressive cyber attack in history where in their financials , movie projects and much more was published publicity by hackers.

What is Cloud Security ?

It is the use of latest technology and security techniques to protect your data , application and infrastructure associated with cloud computing.

Public, Private,Community or Hybrid ?

Cloud Deployment Models

Manufacturing organization has its own private cloud

Manufacturing organization shares cloud with general public

Combination of cloud deployment models

Manufacturing organization shares cloud with other organizations with similar interests

Cloud Security Precautions

- Speaking of passwords, it's crucial that users have strong passwords in place to begin with. We recommend using a password management service, such as LastPass, to store passwords.
- We also recommend changing your passwords regularly for maximum security.
- Companies should ensure employees do not share their account details with anyone as another essential security measure.
- We recommend that any data passed between your company and the cloud is encrypted.
- There are also several third-party encryption tools out there you can use to encrypt files before uploading them, should you prefer to do that.
- Often the best way to ensure cloud security is to test it out. If you are a large organisation with highly sensitive information on the cloud, you can hire ethical hackers to assess how safe it really is.
- Your cloud provider should also be able to offer vulnerability testing, which should be an ongoing process to keep your security up-to-date.

Measures & Controls in Cloud Security

There are four measures and controls are found in the following categories:

- Deterrent Control
- Preventive Control
- Detective Control
- Corrective Control

1) Deterrent Control *:*

- *Deterrent Control is meant to reduce attcak on cloud system, it reduces the threat level by giving a warning sign.*

- If there is an unauthorized access it shows a warning message that there will be adverse consequences if they will proceed further

Measures & Controls in Cloud Security

2) Preventive Control *:*

- *Strengthen the system against any incident or attack by actually eliminating the vulnerabilities.*

- It also prevents unauthorized access so that the privacy of the cloud is not disturbed. Due to this, cloud users are correctly identified

3) Detective Control *:*

- *Detective Control is meant to detect and react instantly and appropriately to any incident.*

- If there is an attack the detective control will inform the user to perform corrective control and address the issue.

Measures & Controls in Cloud Security

4) Corrective Control :

- Corrective Control reduces the consequences of an incident by controlling/limiting the damage.
- It further restores the backup and rebuilds a system so that everything works correctly.

Cloud Security in AWS

Threat Identification is done in 3 stages in the cloud:

1) Monitoring Data.

AWS Cloudwatch

- Monitor Ec2(Amazon Elastic Compute Cloud) and other other AWS resource
- The Ability to monitor custom metrics
- Monitor and store logs
- Views Graphs and Statistics
- To create or set Alarms

Cloud Security in AWS

Threat Identification is done in 3 stages in the cloud:

2) Gaining Visibility

AWS CloudTrail

- CloudTrail is a logging service which can be used to log the history of API calls.
- It can also be used to identify which user from AWS management Console requested the particular service
- Taking reference from our example,this is the tool from where You will identify the notorious 'hacker'.

Cloud Security in AWS

Threat Identification is done in 3 stages in the cloud:

3) Managing Access

AWS IAM

- AWS Identity and Access Management (IAM) is a web service that helps you securely control access to AWS resource for your users.
- Granular permissions
- Secure access to application running on EC2 environment.
- Free to use

Thank You Sir

END