UNIT-V
CLOUD SECURITY

What is Cloud Security?

PROTECTS DATA STORED IN CLOUD COMPUTING ENVIRONMENTS FROM THEFT, DELETION & LEAKAGE.

PROTECTIVE METHODS INCLUDE:

- Access Control
- Firewalls
- Penetration Testing
- Obfuscation
- Virtual Private Networks (VPNs)
- Not Using Public Internet Connections
- Tokenization

CLOUD SECURITY FUNDAMENTALS

- To ensure that the customers does not face any difficulties such as loss of data or data thief.

- Cloud security is the first and foremost concern of every industry and Organization.

- There is a possibility that a malicious user can go through the cloud by impersonating a legal user, Thereby after by infecting the cloud services.

- Most of the vendors are highly concern about the Data integrity , Privacy issues, authentication issue, Data loss, user-level security and vendor level security.

CLOUD RISK

When infrastructure, Applications, Data and Storage are hosted by cloud providers, There is hugh chance of risk in each type of services offering. This is know as cloud Risk.

1. Organizations such as the cloud Security Alliance (CSA) offer certification to cloud providers that will meet their criteria.

2. The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment.

3. **Core Cloud :-** Regardless if you already have a well established cloud security program or are starting your cloud migration for the first time, CSA can help you enhance your security strategy.


Risks of Cloud Computing
Privacy
Availability
Changes
Compliance
www.educba.com

CLOUD RISK DIVISION

A. **Policy and Organizational risks :-**

1. **Lock –in :-** When applications, data and services are dependent on only one cloud providers, it is know as a lock-in problem. There could be SaaS lock-in, PaaS lock-in and IaaS lock-in problems.

2. **Loss of governance** :- This issues comes when the cloud provider may sub-contract or outsource services to third parties (unknown providers) that may not compromise the same guarantees (Such as to provide the service in a lawful way).

3. **Compliance challenges** :- Cloud providers make huge investments for external certifications such as SAS(Statement on Auditing Standard No. 70 (**SAS 70**)) , PCI DSS (PCI DSS, is a formal process used by organizations to identify threats and vulnerabilities that could negatively impact the security of cardholder data)

Compliance challenges continues…

This certifications give them the reputation in the market that they are following the best security practices.

-**However, in some cases particular certification may also be a problem for accessing cloud services.**

- **For example, If a client using AWS cloud wants to use the EC2 (**Amazon Elastic Compute Cloud (Amazon EC2)) and if the EC2 service does not have PCI compliance, then the EC2 service cannot be used for credit card-related transactions.

4. Cloud service termination or failure :- There must be 24x7 support and high availability of all services, but in the competitive world of IT**. Due to lack of financial support and other factors could lead some providers to go out of business or shut down their service offering.** And it is possible that for a short or medium period of time some cloud computing services could be terminated.

5. Supply chain failure :- There is a possibility that the cloud provider could outsource some services to other third parties. In that case, any interruption or corruption in the chain or a lack of coordination of responsibilities between all parties involved can lead to inaccessibility of services, Loss of data confidentially, availability and integrity and reputational losses, because of failure to meet customer demand such as cascading service failure and violating of SLA.

B. TECHNICAL RISKS

1. **Isolation Failure —** This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks).

2. **Resource exhaustions :-** Cloud service is fully on-demand pay-per-use service. There is a chance of risk in proper allocation of resources to cloud users.

3. **Cloud provider malicious insider :-** The malicious actions of an insider could possibly have an impact on the confidentiality, integrity and availability of all kind of data, IP, all kind of services. Taking care of this issue is extremely important in case of cloud computing because cloud architecture contain certain characteristics that are at very high risk.

4. **Intercepting data in transit :-** Cloud services are based on distributed architecture; therefore, transmission of data takes place across multiple physical machines, from one VM to another images distribution between cloud infrastructure and remote web clients, VPN environment and such. This risk is more vulnerable when data is being transferred from one-premises to cloud or cloud storage to on-premises. Spoofing, man-in the middle attacks and sniffing types of attacks could be possible during data transfer-related activities.

5. **Insecure or ineffective deletion of data :-** Whenever a provider is altered,

i. Resources are scaled down
ii. Physical hardware is moved
iii. Data may be available beyond the lifetime specified in the security policy
iv. This may be tough to carry out the procedures stated by the security policy because full data deletion is only imaginable by destroying a disk that also stores data from other clients. When a request to delete a cloud resource is made, this may not result in true wiping of the data. For this true data spreading is required and special procedures must be followed that may not be supported by the standard API.

6**. Conflicts between customer hardening procedures and cloud environment :-** Cloud providers follow different server or instances hardening mechanisms that are little different from traditional server hardening procedures.

7. Loss of encryption Keys :- This includes disclosure of secret keys (e,g file encryption, SSL customer private keys) or passwords to malicious parties. The loss or corruption of those keys or their unauthorized use for authentication and digital signature.

8. Malicious probes or scams :- Malicious probes and scanning, as well as network mapping are indirect threats to the assets being considered. They can be used to collect information in the context of a hacking effort.

9. Compromise service engine :- All cloud providers rely either on an extremely specific platform, or the service engine that is placed just above the physical hardware and manages customers requests at different levels of abstraction.

C. LEGAL RISKS :-

1. **Risk from changes of jurisdiction :-** Customer data may be kept in several jurisdictions, some of which may be high risk. If datacenters are located in high-risk countries (e,g those who lack the rule of law) and enforcement, monocratic police states, states that do not respect international aggreements, sites could be attacked by local authorities.

2. **Licensing risks :-** Licensing conditions such as per-seat agreements and online licensing checks may become unusable in a cloud environment . (For example , software is charged as per instances basis so if our cloud-based instance increases, the cost of the software also increases exponentially.

3. **Data protection risks:-** It can be tough for the cloud customer to efficiently check the data processing that the cloud provider brings out and hence be sure that the data is handled in a lawful way. **There may be data security breaches that are not intimated to the controller by the cloud provider. The cloud provider may misplace control of the data administered by the cloud provider.**

- This issue increases in the case of multiple transfers of data.

OTHER RISKS

1. **Backup lost or stolen :-** This risk is possible due to inadequate physical security procedures, AAA vulnerabilities, User provisioning Vulnerabilities and User de-provisioning vulnerabilities.

2. **Unauthorized access to premises:-** Because of inadequate physical security procedures, unauthorized access in datacenters is possible. Generally cloud providers have large datacenters, therefore, physical control of a datacenter must be stronger because the impact of this issue could be higher.

3. **Theft of Computer equipment :-** This risk is possible because of inadequate physical security procedures. This risk is mainly related to the datacenters.
4. **Natural disasters :-** Natural disasters are possible any time so there must be a perfect disaster recovery plan. Although the risk from natural disasters is quite less compared to traditional infrastructures because cloud providers offer redundancy and fault tolerance by default.

CLOUD COMPUTING SECURITY ARCHITECTURE

There are four layers in the generic architecture of cloud.

1. **Data Center Layer :-** This layer is related to traditional infrastructure security concerns. It consists of Physical Hardware security, theft protection, network security and all physical assets security.

1. **VM layer :-** This layer involves VM level security issues, VM monitoring, Hypervisor-related security issues and VM isolation management issues.

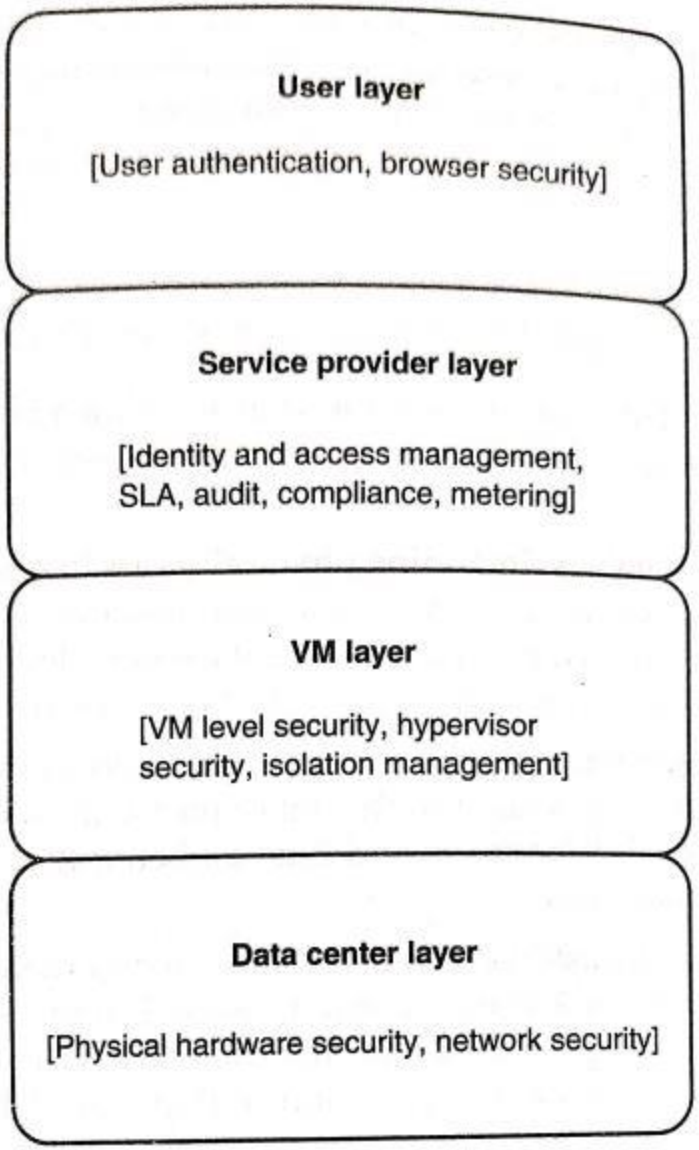

Figure 6.1 | Cloud security architecture.

CLOUD COMPUTING SECURITY ARCHITECTURE

3. Service provider layer :- This layer is responsible for identity and access management , service level agreement (SLA), metering, compliance and audit-related issues.

4. User layers:- This is the first layer of user interaction. It is responsible for user authentication and authorization and all browser-related security issues.

VM SECURITY CHALLENGES

1. **Communication between VMs or between VMs and the Host :-** VMs serve some key requirements for any organization such as the following:-

i. Sharing one physical computer resource among multiple companies or organizations.

ii. Consolidation of different services into one physical computer.

iii. Providing a general hardware platform to host multiple operating system.

2. **VM escape :-** VMs allow us to share the resources of the host computer and provider isolation between VMs and their host.

i. In an ideal situation, any program that runs under the VM should not communicate to any other program inside that or any other VM, but because of some architecture limitations or some other bugs, software affect this isolation.

ii. It may so happen that a program running inside a VM can totally bypass the VM layer and acquire full access to the host system. Such a situation is known as VM escape.

VM SECURITY CHALLENGES

3. VM monitoring from the host:- It is not normally considered a limitation or a bug when one can start monitoring, changing or communication with a VM application from the host. In this case, the host itself starts controlling; therefore the host requires more strict security environments compared to each individual VM.

The host can affect VMs behavior in the following ways

i. **Start, stop, pause and restart VMs.**
ii. **Monitor and configure resources available to the VMs, including CPU, memory, disk and network usage of VMs.**
iii. **Adjust the number of CPUs, amount of memory, amount and number of victuals disks and number of virtual network interfaces to a VM**
iv. **Monitor the applications running inside the VM.**
v. **View, Copy and possibly modify the data stored on the VM's virtual disk.**

4. **VM monitoring from another VM :-** Isolation is a basic characteristic of VM technology; it is usually referred as a security defect when one VM can easily monitor another without defined configuration and privilege to do so.

i. If the hypervisor memory is implemented properly then individual VM protection takes place automatically.

ii. It will not disturb others VMs memory address space. Because VMs do not have direct access to the Host system.

iii. If network traffic is more complicated then there could be an issue with isolation depending on how the network connections are set up with the VMs.

iv. There should be the case of a virtual hub also, if the Vm uses a virtual hub for connecting all VMs host machine, then guest VM my sniff the packets of host VM or other guest VMs using ARP.

5. **Denial of service :-** Because various computing resources like CPU, memory, network and hard disk are shared among multiple VMs and host machine. This may create a denial of service attack against another VM.

6. External modification of a VM: In a business application scenario, users VMs have the privilege of accessing employee databases through a secured application

i. Database security is more critical in a virtual environment.
ii. Database is placed inside a secured VM environment so that any external user is not allowed to access the database outside of the application.
iii. If a VM where database is installed becomes accessible from outside because of a malicious attack, then the database can be corrupted or modified and the system trust can be broken.

7. External modification of the hypervisor :- Because the hypervisor is mainly responsible for the enablement of virtualization while making the process of more self-protected and secure VM, it does not affect the working of any underlying hypervisor. Therefore the first thing is to protect the hypervisor from any external unauthorized access and changes

8. Mixed trust level VMs :- Enterprises must take care of mission critical-related information while leveraging the benefits of virtualization. After applying some self-protection system and some external security mechanism such as integrity checking, file monitoring, log assessment , firewall protection and antivirus detection, The VM can be more secure in mixed environment.

9. Resource contention :- Whenever some resource-consuming operations like malware or antivirus scanning, files and patch updates are executed on VMs, the result of these operations produce high loads on the systems and hamper server applications and VDI environment.

i. To avoid such situations, each VM requires additional significant memory footprint because just like traditional architecture, the antivirus must be installed on each operating system and the same kind of protection is required for each VM too.
ii. More virtualization-sensitive technology is needed for optimal resource utilization and increasing VM performance so that dedicated antivirus and file scanning should not affect the memory footprint on the virtual hosts.

THANK YOU