Unit-5

Cloud Security

Cloud Security Fundamentals

Cloud security is the first and foremost concern of every industry using cloud services. A cloud vendor must ensure that the customer does not face any difficulties such as loss of data or data theft. There is a possibility that a malicious user can go through the cloud by impersonating a legal user, thereby infecting the cloud services and hence affecting various customers sharing the malicious cloud services.

Cloud Risk

When infrastructure, applications, data and storage are hosted by cloud providers, there is a huge chance of risk in each type of service offering. This is known as cloud risk.

Organizations such as the Cloud Security Alliance (CSA) offer certification to cloud providers that meet their criteria. The CSA's Trusted Cloud Initiative program was created to help cloud service provider enable industry-recommended standards, secure access, compliance management, interoperable identity and follow best practices.

Cloud Risk Division

Cloud Risks can be divided into the following four major categories:

1. Privacy and organizational risks
2. Technical risks
3. Legal risks
4. Other risks

Privacy and organizational Risks

1. Lock-in
2. Loss of governance
3. Compliance challenges
4. Cloud service termination or failure
5. Supply chain failure

Technical Risks

1. **Isolation failure:** Multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and even reputation between different tenants. Side channel attacks, SQL injection attacks and guest hopping attacks are example of these.
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:** Malicious insider is **an insider who intends to cause damage to the organization for personal gain**. 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.

4. **Intercepting data in transit:** The data is vulnerable while it is being transmitted. Data can be intercepted and compromised as it travels across the network where it is out of a user's direct control. For this reason, data should be encrypted when in transit. Spoofing, man-in-the middle attacks and sniffing types of attacks cloud be possible during transfer-related activities.
5. **Insecure or ineffective deletion of data:** When it comes to deleting or completely destroying old data from your computer, laptop, hard drive or other media devices, it is vital to keep safety and security the main priorities. Many people and even companies often use unsafe methods to destroy or erase confidential data. Simply deleting or reformatting your computer may not be secure or safe enough. Continuing to practice poor data destruction methods will inevitably lead to identity theft and data breaches.

6. **Loss of encryption keys:** This includes disclosure of secret keys (e.g file encryption, Customer private keys) or passwords to malicious parties, the loss or corruption of those keys.
7. **Compromise service engine:** Cloud provider rely on specific service engine that is placed on top of physical hardware. For IaaS, this can be hypervisor. For PaaS, it can be hosted application. Hacking the service engine may be useful to escape the isolation.

Legal Risks

1. **Risk from changes of jurisdiction:** Customer data may be kept in serval jurisdictions, some of which may be high risk. If datacentres are located in high-risk countries (e.g. Those that lack of rule of law and have an unpredictable legal framework and enforcement, monocratic police states, states that do not respect international agreements), sites could be attacked by local authorities and data or systems subject to enforced disclosure or seizure.
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 at per instances basis so if our cloud based instance increases, the cost of the software also increases exponentially.
3. **Data protection risks** There may be data security branches that are not intimated to the controller by the cloud provider. The cloud customer may misplace control of the data administered by the cloud provider. This issue is increased in the case of multiple transfer pf data.

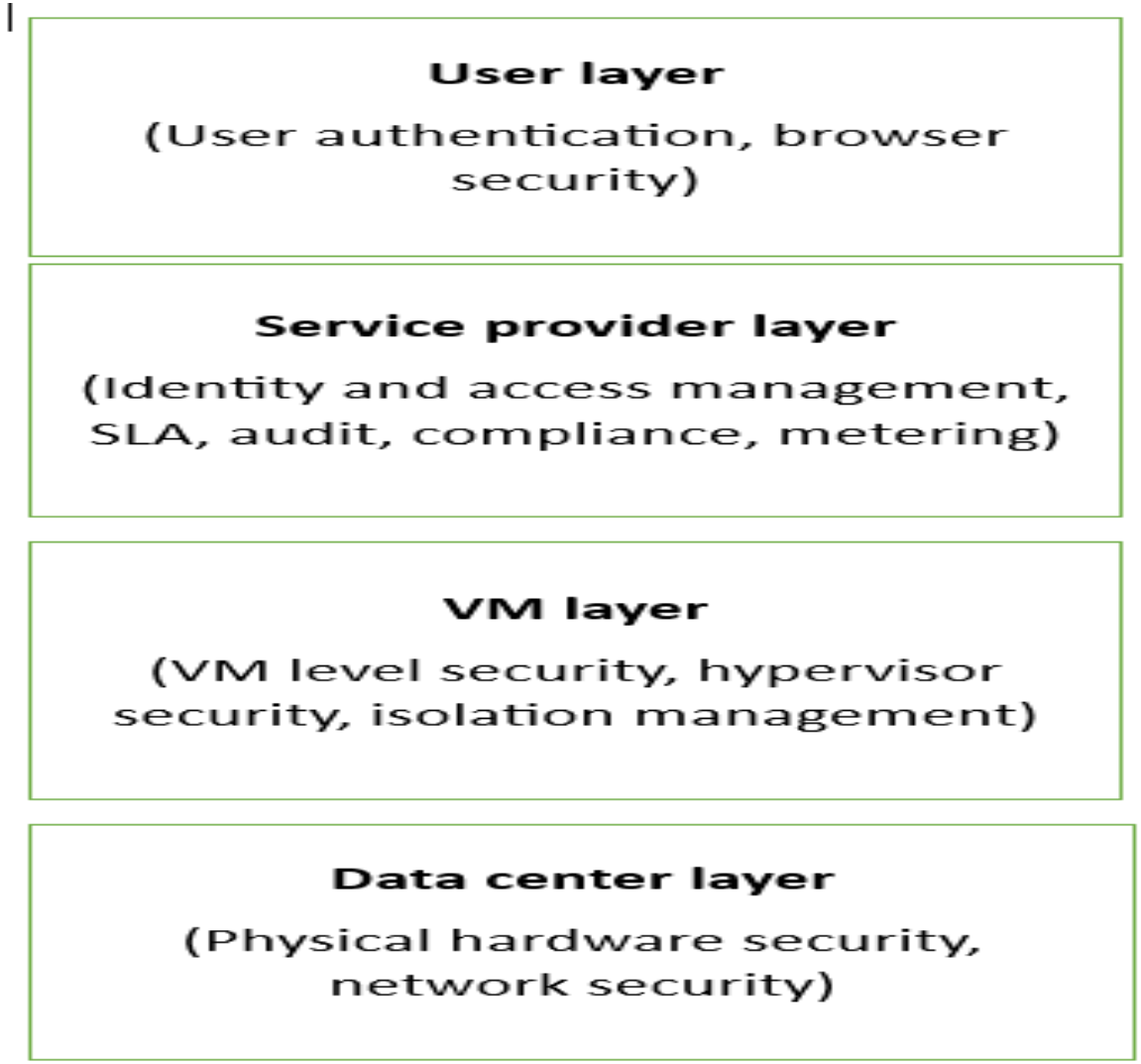
Other Risks

1. **Backup lost or stolen**
2. **Unauthorized access to premises:** Because of inadequate physical security procedures, unauthorized access in datacentres is possible. Generally, cloud providers have large datacentres; therefore, physical control of a datacentre must be stronger because the impact of a breach of this issue could be higher.
3. **Theft of computer equipment:** This risk is mainly related to the datacentre, only authenticated person must be allowed to enter in physical datacentres and dual authentication mechanism should be followed to accesses those machines.
4. **Natural disasters:** Natural disasters are possible any time so there must be perfect disaster recovery plan.

Cloud Computing Security Architecture

Architecture view of the security issues to be addressed in a cloud computing environment for providing security to the customer. This architecture defined four layers on the basis of cloud computing services categorization.

Cloud Computing Security Architecture



- **Data Centre 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.
- **VM Layer:** This layer involves VM level security issues, VM monitoring, hypervisor-related security issues and VM isolation management issues.
- **Service provider layer:** This layer is responsible for identity and access management, service level agreement (SLA), metering, compliance and audit- related issues.
- **User layer:** 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:

- Consolidation of different services into one physical computer.
- Providing a general hardware platform to host multiple operating systems.
- Sharing one physical computer resource among multiple companies or organizations.

2. VM escape:

VMs allows us to share the resources of the host computer and provide isolation between VMs and their host.

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.

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. Because of the host's privileged position, the result may be a total collapse in the security model of the system.

3. VM monitoring from the host:

It is not normally considered a limitation or a bug when one can start monitoring, changing or communicating with a VM application from the host. In this case, the host itself starts controlling; therefore, the host requires more strict security environment compared to each individual VM. The host can affect VMs behaviour in the following ways, although it depends on the kind of VM technology being used.

- Start, stop, pause and restart VMs.
- Monitor and configure resources available to the VMs, including CPU, disk and network usage of VMs.
- Monitor the applications running inside the VM.
- View, copy and possibly modify the data stored on the VM's virtual disks.

4. VM monitoring from another VM:

The hypervisor memory is implemented properly then individual VM protection takes place automatically. It will not disturb other VM's memory address space. Because VMs do not have direct access to the host file systems, VMs should not be able to directly access the virtual disk of each other's VM on the host machine.

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, but if there is a dedicated physical channel for each host VM, then guest VMs should not be able to sniff each other's network packets.

There could be the case of a virtual hub also, if the VM uses a virtual hub for connecting all VMs host machine, then guest VM may sniff the packets of the host VM or other guest VMs using ARP poisoning or some other spoofing technique. Virtualization technology must ensure all possible preventions to such attacks.

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.

This can be avoided by limiting the access of VM resources. There are many virtualization techniques that are used for restricting the allocation of resources to individual VMs. If proper virtualization configuration is implemented, the host machine can prevent denial of service attack among hosts and guest VMs.

6. External modification of a VM:

In a business application scenario, user's VMs have the privilege of accessing employee databases through a secured application. Database security is more critical in a virtual environment. Database is placed inside a secured VM environment so that any external user is not allowed to access the database outside of the application. 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.

This secure VM should be executed by digitally signing every VM and validating the signature before execution. The signing key should be used very carefully and never be placed anywhere else, otherwise it can be compromised.

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 cab be more secure in mixed environments.

9. Resource contention:

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

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.

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.