Day 6

"CLOUD SECURITY"

What is Cloud Infrastructure?

Definition: Cloud infrastructure includes all the hardware (servers, storage, networking) and software required to deliver cloud computing services. It enables organizations to access scalable computing resources on demand without heavy upfront investments.

Architectures:

- Private Cloud: Dedicated to a single organization; secure but costly.
- Public Cloud: Shared via internet; cost-effective but may raise privacy concerns.
- Hybrid Cloud: Combines both; sensitive data stays private, other data on public cloud.

Delivery Models:

- IaaS: Infrastructure only (compute, storage, network); users manage software stack.
- PaaS: Infrastructure + platform (OS, middleware); for app development/testing.
- SaaS: Ready-to-use software apps via web; no local install or maintenance needed.

Cloud Platform and Infrastructure components:

Component	Description
Physical & Environment	Includes data centers, buildings, and surrounding physical infrastructure.
Network	Ensures secure and controlled communication between servers and clients.
Compute	Manages and allocates processing resources (e.g., CPU, memory) for workloads.
Storage	Provides off-site data storage and management on cloud file servers.
Virtualization	Enables virtual environments for compute, storage, and networking resources.
Management	Offers tools/interfaces for configuring and maintaining apps, infra, and platform.

Risk associated with Cloud Platform and Infrastructure:

Risk Category	Examples / Description
Policy & Organizational	- Provider lock-in - Loss of governance - Compliance challenges - Provider exit
General Risks	- Performance failure - Operability issues - Lack of integration/protection
Virtualization Risks	- Guest breakout - Insecure snapshots/images - VM sprawl
Non-Cloud-Specific Risks	- Default passwords - Social engineering - Network attacks
Cloud-Specific Risks	- Management plane breaches - Resource exhaustion - Isolation failure - Insecure deletion
Legal Risks	- Data protection laws - Jurisdictional issues - Licensing & law enforcement

Threats to Cloud Platform & Infrastructure

1. Natural Disasters
   Risk: Fire, floods, earthquakes can damage infrastructure.
   → Mitigate using risk assessment tools and disaster recovery planning.

2. Unauthorized Physical Access
   Risk: Intruders can access and damage hardware.
   → Use physical security controls and risk mitigation strategies.

3. Employee Negligence
   Risk: Accidental deletion, mishandling logs.
   → Apply a strong security policy and training.

4. Privilege Escalation
   Risk: Attackers compromise VMs via hypervisor.
   → Use patched hypervisors and access control policies.

5. Insecure Data Deletion
   Risk: Residual data may persist after deletion.
   → Ensure secure wipe of storage and hardware reallocation.

6. Obsolete Cryptography
   Risk: Weak or outdated encryption protocols.
   → Enforce modern cryptographic standards.

7. Cloud Service Failure
   Risk: Attackers disable services.
   → Use multiple IDS systems for intrusion prevention.

8. Insufficient Monitoring & Logging
   Risk: Hard to trace incidents or user activity.
   → Use advanced logging tools and audit trails.

9. Third-party Supplier Failure
   Risk: Outsourced vendors may have weak security.
   → Vet suppliers carefully and maintain backup vendors.

10. Vendor Lock-in
    Risk: Difficult to switch cloud providers.
    → Evaluate CSPs beforehand and understand migration costs.

11. Subpoena & e-Discovery Risks
    Risk: Varying data privacy laws across countries.
    → Be aware of the legal jurisdiction of your CSP.

--The End--