**Day 25**





**“CLOUD SECURITY”**

**What is a Cloud Application?**

A cloud application is internet-based software deployed in a cloud environment, accessed through browsers or APIs. Data and processing are handled by remote cloud servers, while users interact via web or mobile interfaces. Examples: Google Docs, Microsoft 365.

**Deployment Models:**

1. **Public Cloud** – Services open to anyone.  
   *Advantages:* cost-efficient, scalable, reliable, no maintenance.
2. **Private Cloud** – Used by a single organization, stays behind a firewall.  
   *Advantages:* secure, flexible, controlled, scalable.
3. **Hybrid Cloud** – Mix of public + private.  
   *Advantages:* balance of control, flexibility, and cost-efficiency.

**Advantages of Cloud Applications:**

* **Reliability:** High availability, disaster recovery.
* **Scalability:** Dynamic, instant scaling.
* **Cost Efficiency:** Pay-as-you-go, no infrastructure investment.
* **Ease of Management:** Cloud Management Platforms (CMPs) via APIs.
* **Security & Data Sharing:** Centralized, backed-up, world-class protections.
* **APIs:** Enable integration and predictable development.
* **Agility:** Faster updates, testing, and response to business needs.

**Disadvantages:**

* **Security Risks:** Continuous monitoring needed.
* **Downtime:** Dependent on internet & provider outages.
* **Lack of Control:** CSP owns/operates infrastructure.

**Security Benefits of Cloud Applications:**

* **High Baseline Security:** Providers meet regulatory & compliance standards.
* **Responsiveness:** APIs/automation enable quick security updates (e.g., firewall rules).
* **Isolated Environment:** Virtual networks prevent lateral attacks.
* **Independent VMs:** Microservices reduce attack surface.
* **Elasticity:** Autoscaling with immutable servers reduces admin risks.
* **DevOps Security:** Automation strengthens code hardening & app security.
* **Unified Management:** APIs give full-stack visibility & monitoring.

**What is Cloud Application Security?**

Application security = measures to protect data/code within apps, covering design, development, and post-deployment.

* Focus: securing SaaS, PaaS, IaaS application layer.
* Prevents vulnerabilities: XSS, SQL injection, CSRF, poor authentication/session handling.
* Part of **zero-trust security** to protect frequent cloud app access.

**Why Cloud Application Security is Needed?**

* Identifies apps in use & employee access levels.
* Protects distributed organizational data across cloud apps.
* Ensures security compliance by mitigating cloud threats.

**Cloud Application Security Threats & Solutions**

| **Threat** | **Solution** |
| --- | --- |
| Incorrect setup | Logging, segmentation, audits |
| Unauthorized access | Access controls, business partnerships |
| Insecure APIs | Authentication, encryption, monitoring |
| Account hijacking | MFA, IP restrictions |
| App vulnerabilities | Web Application Firewalls (WAFs) |
| Bad bots | IP reputation, signature DBs |
| App-layer DDoS | Application Delivery Controllers (ADCs), load balancing |
| Data breaches | Data recovery plan, vendor backup checks |

**Security Challenges of Cloud Applications**

1. **Limited Visibility:** Logging/monitoring reduced in PaaS; less transparency for users.
2. **Increased Application Scope:** Management plane security is critical; multi-access risks sensitive data exposure.
3. **Changing Threat Models:** Must adapt to provider’s shared security model & response processes.
4. **Reduced Transparency:** External integrations hide app processes, reducing visibility.

--The End--