Threats and Vulnerabilities Associated with Operating in the Cloud

Chapter 6

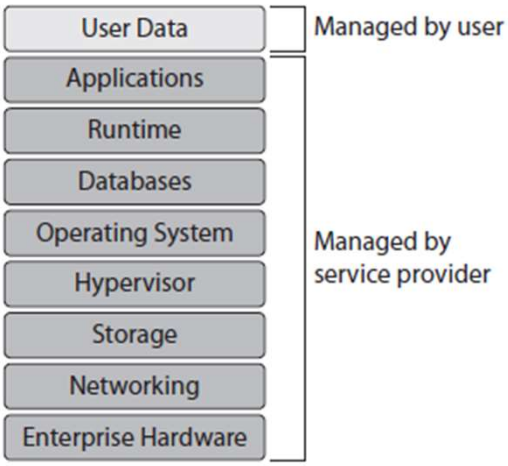
Episode 6.01

Cloud Models

Objective 1.6 Explain the threats and vulnerabilities associated with operating in the cloud.

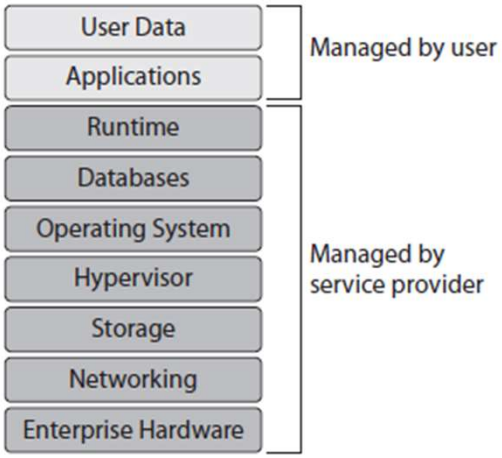
- Cloud service models
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
- Cloud deployment models
  - Public
  - Private
  - Community
  - Hybrid

Software as a Service (SaaS)



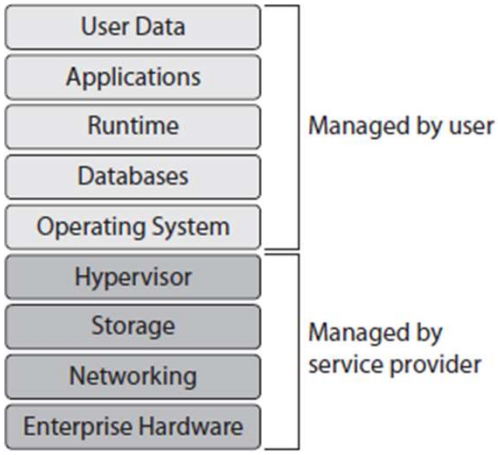
Source: Chapman, B., & Maymí, F. (2020). *CompTIA CySA+™ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)*, 28.

Platform as a Service (PaaS)



Source: Chapman, B., & Maymí, F. (2020). *CompTIA CySA+™ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)*, 28.

Infrastructure as a Service (IaaS)



Source: Chapman, B., & Maymí, F. (2020). *CompTIA CySA+™ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)*, 28.

Cloud Deployment Models

- Public
  - Most popular
  - Lease connectivity and functionality from service provider
- Private
  - Create collection of servers in your own data center
  - Only for internal network users
- Community
  - Private cloud owned by a consortium
  - Shared among many entities
- Hybrid
  - Looks like single cloud but made up of both public and private (and maybe community)
- Each model opens up vulnerabilities
  - Authorization concerns
  - Authentication concerns

Episode 6.02

Remote Service Invocation (FaaS, IaC, API)

Objective 1.6 Explain the threats and vulnerabilities associated with operating in the cloud.

- Function as a Service (FaaS)/serverless architecture
- Infrastructure as code (IaC)
- Insecure application programming interface (API)

Function as a Service (FaaS)

- Serverless architecture
  - No servers need to be set up
  - Focus is on responding to functionality requests
- Example: Amazon Lambda

Infrastructure as Code (IaC)

- Developers tend to develop based on personal preferences
  - Development environments diverge
  - Can introduce vulnerabilities
- Structured method to create stable development environments
- Minimizes local configuration differences
- Virtualization and structured provisioning
  - Makes it easy to create cloned environments

Insecure Application Programming Interface (API)

- Poorly written APIs may have vulnerabilities
- OWASP API Security Project top ten vulnerabilities
  - Broken object level authorization
  - Broken user authentication
  - Excessive data exposure
  - Lack of resources and rate limiting
  - Broken function level authorization
  - Mass assignment
  - Security misconfiguration
  - Injection
  - Improper asset management
  - Insufficient logging and monitoring

Episode 6.03

Cloud Vulnerabilities

Objective 1.6 Explain the threats and vulnerabilities associated with operating in the cloud.

- Improper key management
- Unprotected storage
- Logging and monitoring
  - Insufficient logging and monitoring
  - Inability to access

Improper Key Management

- Encryption can protect
  - Confidentiality
  - Integrity
  - Non-repudiation
- Security depends on the encryption key
- Key management is difficult (to do right)
  - Generation
  - Distribution
  - Replacement

Unprotected Storage

- Cloud storage is located on someone else's computing systems
  - Be sure to secure the storage
  - Vulnerabilities can leave storage open to hackers
- Admins must configure security settings properly
- Common loophole is mass access
  - Often granted for convenience
  - May expose sensitive data

Logging and Monitoring

- Responsibility changes based on cloud service models
- If service provider is taking on most of the responsibility, user has little control over what gets logged
- Monitor and log all important events
- More services means less granular control
- SLAs spell out roles and responsibilities