Cloud Platform and Infrastructure Security

CCSP Series - Chapter # 3

Cloud Platform and Infrastructure Security Overview

Introduction to Cloud Security

- Understanding architecture for various cloud models
- **Key components:** Physical, Services, Communication
- Shared Security Responsibility Model

Shared Responsibility in Cloud Security

Security Division in Cloud Computing

- **CSP Responsibilities:** Platform, Physical Security, Managed Components
- **Customer Responsibilities:** Data, Access Management, Client-side Protection
- Importance of Clear Understanding of Duties

Role of a Cloud Security Professional

Strategic Functions for Business Objectives

1. Ensure Business Continuity and Disaster Recovery

2. Streamline Scalable Architecture for Demand

3. Leverage Cloud for Cost Savings & New Business Models

Components of Cloud Infrastructure

Core Components Across Cloud Service Models

Physical Environment: Location of CSP's Data Centers

Network & Communications: Securing Data Transference

Compute Resources: Management of Virtual and Physical Resources

Physical Environment Security Needs

Types of Clouds & Their Physical Security

1. **Private Cloud:** Organization's own premises or virtualized through Major CSPs.

2. **Community Cloud:** Hosted and physically secured by a community member.

3. **Public Cloud:** Commercial vendor like AWS, Azure provides & manages physical security.

Ensuring Cloud Network Integrity

Guaranteeing Security Between Customer & CSP

Deployment of Secure Protocols like HTTPS

Encryption of Data in Transit: VPNs and Cryptographic Methods

Firewalls and Secure Communication Systems

Cloud Compute Resource Security

Security Aspects in Computing

- **Customer's Role:** Data Integrity and User Management
- **CSP's Role:** Maintenance & Security of Physical and Virtualization Components
- **Service Models Impact on Responsibilities:** IaaS, PaaS, SaaS Explained

Virtualization in Cloud Computing

Types and Security of Hypervisors

1. Type 1 (Bare-Metal) and Type 2 (Hosted)

2. **Criticality of Hypervisor Security:** Prevention of Unauthorized Access

3. **CSP's Duty:** Update and Maintain Virtualization Environment Safely

Securing Cloud Storage

Cloud Storage Security Challenges

CSP's Role: Physical Protection & Maintenance

Customer's Role: Configuration, Encryption Management, and Data Privacy Control

Strategies for Effective Storage Security & Data Lifecycle Management

Management Plane Security

Protecting Cloud Environment Configuration Access

- Importance of Root/Administrative Account Protection
- **IAM Tools:** MFA, RBAC/ABAC, Logging User Actions
- Vendor-specific Management Tools & Best Practices

Designing Secure Cloud Data Centers

Considerations for Secure Cloud-based Facilities

1. Logical Data Center Design & Secure Configuration
2. Tenant Partitioning & Robust IAM for Cloud Resources
3. **Impact:** Environment, Physical Design, Connectivity

Risks in Cloud Infrastructures & Platforms

Identifying and Analyzing Cloud-related Risks

Risk Frameworks Applicability: ISO/IEC 31000:2018, NIST SP 800-37

Specific Cloud Risks: Data Control, Multitenancy, Vendor Policies

Essential Metrics: RTO, RPO, and Recovery Service Levels

Mitigating Cloud-Related Risks

Implementing Effective Cloud Security Controls

- Selection of Qualified CSP based on Needs and Risks
- **Data Encryption:** For Data at Rest and in Transit
- **Utilization of CSP Tools:** AWS Inspector, CloudWatch for Secure Computing

BCP & DRP in Cloud Environments

Incorporating Cloud Solutions in Continuity Strategies

1. **Business Continuity Plan (BCP):** Maintaining Operation Post-Disruption
2. **Disaster Recovery Plan (DRP):** Restoring Normal Operations
3. Utilizing Cloud's Native High Availability and Scalability Features

Summary and Best Practices for Cloud Security

Maximizing Cloud Security

Embracing Shared Security Responsibility & Precise Configuration

Understanding Cloud Resource Management for Optimal Security

Regular BCP & DRP Testing for Robust Preparedness

Information Security Buzz

Discover more at our InfoSec Knowledge Hub