Chapter 8

Cloud Security

Episode 8.01

Cloud Security

Company Security Policies

- Documented plan and agreement that includes:
  - Rules
  - Regulations
  - Course of action

Why Create Security Policies?

- Maintain desired level of security
- Uphold compliance
- Legal protection
- Asset documentation
- Procedural continuity
- Authority

Policy Tasks

- Obtain management support
- Perform risk assessment and impact analysis
- Document and define vulnerabilities and countermeasures
- Plan response, forensics, enforcement, and reporting
- Communications and training of users and staff
- Provide ongoing monitoring and auditing
- Review and revision process

Quick Review

- A security policy is a documented plan and set of requirements for secure use of a system
- Security policies are often implemented to ensure compliance with government and industry regulations
- It is essential to have management support for effective security policy enforcement

Episode 8.02

Standards and Compliance Demo

Compliance and Audit Requirements

- Laws and regulations
  - Privacy laws
  - Data retention laws
  - Healthcare information laws
  - Payment processing guidelines

Compliance and Audit Requirements

- Data classification is a common compliance requirement
  - Enables authorization
  - Enables confidentiality
  - Enables life cycle management
  - Ex: Top Secret, Secret, Unclassified

Quick Review

- HIPAA is an example of a privacy regulation and is imposed on organizations in the United States dealing with health information
- Laws exist in various countries related to privacy, data retention, healthcare, and payment processing
- Data classification may be a compliance requirement

Episode 8.03

Data Security and Compliance Controls

Records Management

- Versioning
- Retention
- Destruction
- Write once read many
- Laws and regulations (legal hold)

Encryption

- Data privacy regulations
- Industry standards
- Contractual obligations
- Government regulations

Integrity

- Data privacy regulations
- Industry standards
- Contractual obligations
- Auditing and reporting requirements

Classification

- The process of categorizing, tagging, or describing data based on sensitivity, importance, and or the level of protection required
- Classification use cases include:
  - Access controls
  - Data protection
  - Retention policies
  - Compliance requirements
  - Incident response

Segmentation

- The process of dividing a computer network into smaller sub-networks or segments
- Segmentation can provide security and compliance
  - Access control
  - Risk management
  - Compliance enforcement
  - Monitoring and detection

Data Loss Prevention (DLP)

- A set of tools, policies, and procedures used to prevent the loss or theft of sensitive data
- DLP can be used for security and compliance:
  - Compliance with data privacy regulations
  - Protection of intellectual property
  - Prevention of data breaches
  - Protection of financial data
  - Risk management

CASB

- Cloud Access Security Brokers (CASBs) provide visibility and control over the use of cloud services
  - Data protection
  - Access control
  - Compliance
  - Threat detection and response

Episode 8.04

Identity, Authentication, and Authorization

Identity and Identification

- A person, device, or service may be considered an entity associated with an identity in an identity management system (IMS)
  - Active Directory is an example of an IMS

Identity and Identification

- Identification is the process of presenting an identity
- Authentication is the process of validating ownership of that identity
  - The entity is the identity it claims to be
- Identities are typically tracked with accounts
  - An account life cycle management process should be implemented
  - Upon failed authentication, the account may be locked

AAA

- Authentication
- Authorization
- Accounting

Authentication Methods

- Local authentication
- Federated authentication
  - Trusted authentication
  - Single Sign-On (SSO)

Authentication Methods

- Something you are
  - Thumb scanner
- Something you have
  - Smart card
- Something you know
  - Password/PIN

Account Authorization

- Once authenticated, the entity must be authorized to perform actions or access resources
- Authorization is the process of validating the rights of the entity
  - Access control lists (ACLs)
  - Permissions

Quick Review

- Authentication is the process of validating ownership of an identity
- AAA stands for authentication, authorization, and accounting
- Authentication methods include local authentication, federated authentication and single sign-on (SSO)

Episode 8.05

Multi-Factor Authentication Lab

Quick Review

- Multi-factor authentication uses more than one proof of identity
- Common factors include passwords, PINs, smartcards, certificates, tokens, thumb scanners, etc.
- Cloud providers work with software-based token systems so that you can receive a token validation number on your mobile phone for authentication

Episode 8.06

Identity and Access Management Solutions

Identification and Authentication

- Identification and Authorization
  - Identification: Who or what is it?
  - Authorization: What can the identity do or access?

Directory Services

- A centralized database exposed through a service for authentication and authorization
  - User management
  - Group management
  - Resource management
- AWS Directory Service
- Google Cloud Directory
- Azure Active Directory

Public Key Infrastructure

- Used to deploy and manage certificates
- Involves one or many servers
- Used for cloud solutions:
  - Secure communication
  - Authentication and access control
  - Secure data storage
  - Secure transactions

Certificate Management

- Certificate issuance
- Certificate revocation
- Certificate renewal
- Certificate validation
- Key management
- Certificate backup and recovery
- Compliance reporting

SAML

- Security Assertion Markup Language
  - XML-based
  - Used to exchange authentication and authorization data
  - Allows for single sign-on (SSO)
  - Often used with CSPs for federated identity
  - May be used with email, file access, application access, and more

Secret/Key and OTP

- Secret or Key (Secret/Key) elements are used to encrypt/decrypt data and for authentication
- One Time Password (OTP) is used for a single authentication transaction

Episode 8.07

Authorization Lab

Objects Requiring Authorization

- Resources
  - Things that you can consume/use
- Processes
  - Takes action in the computer
  - Usually impersonates a user/group
- Users and groups
- Cloud systems
  - Compute
  - Network
  - Storage
- Cloud services

Access Control Methods

- Discretionary Access Control (DAC)
  - The users can manage permissions
- Non-discretionary Access Control (NAC)
  - Only administrators can manage permissions
- Mandatory Access Control (MAC)
  - Permissions are required for all objects
- Role-Based Access Control (RBAC)
  - Permissions are granted based on roles

Quick Review

- Resources, such as files and folders, as well as processes should use authorization
- Cloud systems, such as compute, network, and storage, should also use authorization
- Mandatory access control (MAC) requires that all objects use authorization

Episode 8.08

Encryption Demo

Choosing an Encryption Solution

- At rest
  - Whole drive
  - Individual files
- In transit
  - VPNs
    - IPSec is common
  - SSL/TLS
    - Used with HTTP and FTP

Choosing an Encryption Solution

- At rest
  - Whole drive
  - Individual files
- In transit
  - VPNs
    - IPSec is common
  - SSL/TLS
    - Used with HTTP and FTP

Common Ciphers

- Advanced Encryption Standard (AES)
  - Block
- RC4
  - Streaming
- Symmetric ciphers
  - Same key to encrypt and decrypt
- Asymmetric ciphers
  - Separate keys to encrypt and decrypt
  - Public key and private key
  - Public key cryptography
    - Implements asymmetric ciphers
    - Validates the sender's identity
    - May require a Public Key Infrastructure (PKI)

Quick Review

- At rest encryption encrypts data in storage
- In transit encryption encrypts data during network transmission
- AES is the commonly deployed encryption solution for at rest encryption and in many in transit solutions as well

Episode 8.09

Encryption Solutions

Encryption Levels

- Application
- OS
- Storage
- Filesystem
- Network

Tunnels

- The encapsulation (bundling) of one protocol inside another protocol
  - Add encryption and you have a VPN
- Tunneling solutions:
  - Secure Shell (SSH)
  - Layer 2 Tunneling Protocol (L2TP)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Generic Routing Encapsulation (GRE)

Encryption Protocols

- IPSec
- Transport Layer Security (TLS)
- Hypertext Transfer Protocol Secure (HTTPS)

Episode 8.10

Compute Security Demo

Compute Implementations

- Serverless
  - Access permissions are sufficient
  - Functions
- Virtual servers (instance)
  - All traditional security solutions used on local physical servers

Hardening a Cloud Instance

- Disable unneeded ports
- Manage local accounts with best practices
  - Disable, deactivate, or remove default accounts
- Patch or update the OS
- Patch or update the applications
- Install anti-virus/anti-malware software
- Implement host-based/software firewalls

Quick Review

- Serverless computing is typically implemented as accessible functions
- Unneeded ports should be disabled on all virtual servers
- An update or patch procedure should be defined for all cloud compute instances

Episode 8.11

Account Management Lab

Quick Review

- After some number of failed login attempts accounts should be locked
- Passwords complexity is implemented with multiple character types and length requirements
- Accounts that are no longer required should be deleted or disabled

Episode 8.12

Segmentation Lab

Segmentation

- Network
  - Separate virtual private clouds
  - Subnets within a virtual private cloud
- Storage
  - Different physical locations/regions
  - Separation based on content to restrict access
- Compute
  - Different instances do different compute processes

Quick Review

- Network segmentation is used to separate sections of the network
- Storage segmentation is used to separate one storage system from another
- Compute segmentation is used to separate processes by using multiple instances

Episode 8.13

Security Tools Demo

Security Tools

- APIs (Application Programming Interfaces)
  - Have code that can be called upon by other applications
  - Get results

Security Tools

- Vendor applications
  - 3rd party tools you can use in the cloud
  - Come with security features built in
  - Keep in mind minimum requirements
    - Authentication
    - Authorization
    - Accounting
- CLI (command-line interface)

Security Tools

- Web GUI (graphical user interface)
  - Web-based GUI interface with access to security functions
  - May or may not be cloud provider's portal
  - Might be 3rd party tool

Security Tools

- Cloud portal
  - Cloud provider's specific web GUI
  - Manage everything related to your cloud

Security Tools

- Scope of impact
  - Understand what you're doing when you're doing it
  - Especially important with CLI
    - Analyze the command you're about to execute
    - What all is it going to impact?
  - Manage everything related to your cloud

Quick Review

- APIs may be made available for security management with scripting
- Command line interface (CLI) tools can be used for security management
- Security tools may impact a single service, server, subnet, or the entire cloud deployment

Episode 8.14

Security Services

Firewalls

- Port-based
  - Configure allowed/disallowed ports
  - IP address filtering
- Stateful
  - Allows incoming connections based on internal requests

Firewalls

- In the cloud
  - Implement in the cloud just like a local network
  - Service from cloud provider (Firewall as a Service)
  - Install virtual server instance
    - Connect a network adapter at each subnet
    - That server can act as a full-scale firewall

Essential Services

- Antivirus
- Anti-malware
- IDS/IPS
- Host-based IDS/IPS
  - Runs on local machines
  - Looks for attacks

Quick Review

- Port-based firewalls control traffic flow by filtering TCP and UDP ports
- Anti-malware tools include antivirus, anti-spam, and other services
- Host-based IDS solutions run on individual computer nodes to detect intrusion attempts against that node

Episode 8.15

Additional Network Security Solutions

DNS Security

- DNS Security (DNSSEC)
- DNS over TLS (DoT)
- DNS over HTTPS (DoH)

Network Time Protocol

- NTP is used to synchronize clocks for computing devices
  - Network devices synchronize with one or more NTP servers
  - NTP servers can synchronize with Internet-based time servers
    - time.google.com
    - pool.ntp.org
    - time.windows.com

Firewalls and Other Devices

- Firewalls
- Stateful and stateless
- Filtering
- Rules
- Web Application Firewall (WAF)
- Application Delivery Controller (ADC)
- Packet Brokers

Network Access Control

- NAC enforces security policies on devices attempting to access a network
  - Authenticates and authorizes devices
- NAC can be used for many benefits:
  - Prevent unauthorized network access
  - Enhance security posture
  - Comply with regulations
  - Monitoring and reporting
  - Guest access

Network Flow Control

- Network flows
- Log monitoring
- Event monitoring

Episode 8.16

Network Hardening

Network Hardening Basics

- The process of securing computer network resources to reduce vulnerability
- Network hardening process:
  - Inventory assets
  - Assess risks
  - Configure for security
  - Implement access control
  - Monitor and audit
  - Respond to incidents

OS Hardening

- Disable unneeded services and applications
- Apply security patches and updates
- Configure user accounts and permissions
- Implement strong passwords and authentication
- Configure firewalls, endpoint security, etc.
- Enable logging and monitoring
- Implement encryption

Device/Component Hardening

- Change default passwords
- Disable unused ports and services
- Apply security patches and updates
- Configure access controls
- Enable logging and monitoring
- Implement encryption
- Enable two-factor authentication

VLANs

- Basic VLANs (Virtual Local Area Networks)
- VXLAN (Virtual Extensible LAN)
- GENEVE (Generic Network Virtualization Encapsulation)

Micro-Segmentation

- Divides a network into very small segments
- Reduces the attack surface of each segment
- Each segment is isolated from the others
- May be implemented using virtual firewalls, ACLs, and SDN controllers
- Often said to apply to “east/west” traffic flows

Tiering

- Dividing resources, systems, or applications into levels (tiers) of importance or sensitivity
- Apply varying levels of security control to each tier
- Multi-tier web applications are common examples
- May be used in network segmentation as well

Episode 8.17

Application and OS Security

User Permissions

- A set of access control rules that allow or disallow access or rights to resources or processes
- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

Endpoint Security

- Antivirus/anti-malware
- Endpoint Detection and Response (EDR)
- Host-based IDS/IPS (HIDS/HIPS)/software firewall
- Hardened baselines
- File integrity
- Log and event monitoring
- Configuration management and builds

Policy-Based Management

- A method for managing IT resources (cloud resources)
- Helps in the following ways:
  - Establish consistent security controls across cloud environments
  - Ensure compliance with regulatory requirements
  - Detect and respond to security threats in a timely manner
  - Reduce the risk of data breaches and cyber attacks

Episode 8.18

Security Automation and Orchestration

Automation

- Used to generate actions without intervention or without full interaction by admin
- Usually about a task, not large-scale actions
- User management
  - User account creation
  - User account removal
  - User account disablement
  - Permission settings
  - Resource access
- Implemented with scripting or custom programming against cloud APIs

Orchestration

- Causes several interdependent tasks to occur without interaction
  - Creating entire server farms
  - Generating multiple databases
  - Creating users, groups, roles, permissions and other security settings

Orchestration

- Driven by policies
  - Define the policies
  - Execute tasks
  - Tasks are performed based on policies

Scope of Impact

- Always consider the impact of automation and tools in relation to security requirements
  - Will the tools comply with policies?
  - Will the tools comply with regulations?
  - Can the solution be automated/orchestrated without breaking security best practices?

Quick Review

- User account management is a frequently automated security task
- Orchestration is used to perform large-scale automation
- Scope of impact must be considered with any automation but especially with orchestration

Episode 8.19

Models and Security

Cloud Service Models and Security

- SaaS (Software as a Service)
  - Who has access?
  - What can they do?
- PaaS (Platform as a Service)
  - Right people have access to test/run/ deploy code
  - Users can run the code

Cloud Service Models and Security

- IaaS (Infrastructure as a Service)
  - Right people have access to cloud management
  - Right people have access to develop
  - Right people have access to run the applications
- XaaS (Everything as a Service)
  - It. Depends.

Cloud Deployment Models and Security

- Public/community
  - SaaS/PaaS/IaaS security applies
- Private
  - Extra layer of physical security to consider
- Hybrid
  - Cloud and non-cloud security to consider

Quick Review

- Managing SaaS security is about access permissions and, in some cases, authorization
- IaaS requires management or cloud management access as well as access to resources
- Private and Hybrid cloud solutions require all traditional security considerations because they run on the local network

Episode 8.20

Risk and Reward

Scanners

- Port scanners
  - Examples include Nmap, Masscan, and Angry IP Scanner
- Vulnerability scanners
  - Examples include Nessus, OpenVAS, and Qualys

Vulnerability Assessment

- Default and common credential scans
- Credentialed scans
- Network-based scans
- Agent-based scans
- Service availabilities

Patch Prioritization

- Patch types:
  - Hot fixes
  - Virtual patches
  - Signature updates
  - Rollups
- Scheduled updates and prioritization

Cloud-Specifics

- Cloud service models impact security implementation
  - Saas
  - PaaS
  - IaaS
- Security tools impact systems and services
  - Performance
  - Integration
  - Maintenance and Cost

Risk Register

Risk	Likelihood	Impact	Mitigation/Management
Unauthorized access to video files	High	High	Implement multi-factor authentication and encryption to protect against unauthorized access. Conduct regular security audits and penetration testing to identify vulnerabilities.
Loss of video files due to system failure	Medium	High	Implement backup and recovery procedures to ensure that video files can be recovered in the event of a system failure. Test backup and recovery procedures regularly to ensure they are effective.
Data privacy violations	Low	High	Implement data privacy controls to protect against unauthorized access, use, and disclosure of personal information. Ensure compliance with data privacy regulations such as GDPR and CCPA.
Poor performance of AI engine	Medium	Medium	Conduct performance testing to identify and address potential performance issues. Monitor system performance regularly and optimize system resources as needed.

Create a Risk Register

- Identify potential risks
- Assess likelihood and impact
- Prioritize risks
- Develop mitigation or management strategies
- Document the risk register
- Review and update regularly

Episode 8.21

Incident Response (IR)

Incident Response

Incident response is the **process** of **preparing** for, **detecting**, **analyzing**, **containing**, and **recovering** from **security incidents** in computing systems, network systems, and other technology environments. *Security incidents* can include a wide range of events, such as **cyber attacks**, **malware infections**, **unauthorized access**, **data breaches**, and other types of **security breaches**.

IR Preparation

- Documentation
- Documented incident types/categories
- Call trees
- Training
- Tabletops
- Roles and responsibilities

IR Procedures

- Identification
  - Scope
- Investigation
- Containment, eradication, and recovery
  - Isolation
  - Evidence acquisition
  - Chain of custody

Post Incident

- Lessons learned exercises
  - Log analysis
  - Root cause analysis
  - Configuration management
  - Policy and procedure analysis