B.Tech, 6^{th} Sem., Computer Networking: Security(CLASS NOTE)

Dr. Laxmidhar Biswal

May 15, 2025

Compare and contrast security implications of different architecture models

Dr. Laxmidhar Biswal

Introduction/Motivation

Given a scenario, apply security principles to secure enterprise infrastructure

Objectives of this chapter

- Focuses on applying security principles in enterprise infrastructure.
- Emphasizes device placement and security zones to isolate data and reduce risk.
- Covers various security appliances, including types of firewalls and their appropriate use cases.
- Reviews methods of secure communication, access control, and selection of secure controls.

Given a scenario, apply security principles to secure enterprise infrastructure

Enterprise Infrastructure Security

- Holistic Security Approach:
  - Align security with business goals.
  - Assess risk profile and evolving threats.
  - Embrace defense-in-depth with layered protections.
  - Foster a security culture through vigilance and continuous learning.
- Device Placement:
  - Divide network into LAN (trusted), DMZ/screened subnet (boundary), and WAN (untrusted).
  - Use firewalls to filter traffic between zones.
  - Strategic device placement (e.g., intrusion detection system/intrusion prevention system, proxy servers, routers, jump servers) strengthens security.

Given a scenario, apply security principles to secure enterprise infrastructure

Dr. Laxmidhar Biswal

Enterprise Infrastructure Security

- Security Zones:
  - Segmentation: Divide network based on data sensitivity, user roles, or device types.
  - Access Control: Implement strict access policies per zone.
  - Data Protection: Use Full Disk Encryption, VPNs, and DLP tools.
  - Monitoring: Apply SIEM(Security Information and Event Management) and SOAR(Security Orchestration, Automation, and Response) for real-time threat detection.
  - Isolation: Limit lateral movement of attackers.
  - Compliance: Align with frameworks like HIPAA (Health Insurance Portability and Accountability Act), PCI DSSPCI DSS (Payment Card Industry Data Security Standard).
  - Efficiency: Easier management and faster incident response.
  - Defense-in-Depth: Multiple layers of security to delay/deter attackers.

Given a scenario, apply security principles to secure enterprise infrastructure

Enterprise Infrastructure Security

- Attack Surface: Components: Endpoints, network services, ports, credentials, cloud services, and users.
- Minimization Techniques:
  - Regular vulnerability assessments.
  - Strict access control and MFA (Multi-Factor Authentication).
  - Network segmentation.
  - Patch management.
  - Security awareness training.
  - Avoid single points of failure.

Given a scenario, apply security principles to secure enterprise infrastructure

Enterprise Infrastructure Security

- Connectivity:
  - Scalability: Design for growth.
  - Security: Integrate security into all connections.
  - Redundancy: Use failover mechanisms.
  - Complexity: Manage various devices and technologies.
  - Remote Work: Ensure secure and seamless remote access.
- Failure Modes:
  - Fail-Closed: Blocks access on failure; enhances security.
  - Fail-Open: Allows access on failure; risks exposure.

Given a scenario, apply security principles to secure enterprise infrastructure

Enterprise Infrastructure Security

- Device Attributes:
  - Active Devices: Take immediate actions (e.g., firewalls, IPS).
  - Passive Devices: Monitor traffic (e.g., IDS).
  - Inline Devices: Directly control traffic flow (e.g., firewalls, load balancers).
  - Tap/Monitor Devices: Observe without interfering (e.g., packet analyzers).

Given a scenario, apply security principles to secure enterprise infrastructure

Enterprise Infrastructure Security

- Defense-in-Depth:
  - Layered security approach to delay and complicate intrusions.
  - Combines physical, technical, and administrative safeguards.
- Security Culture:
  - Promote vigilance, continuous learning, and proactive defense across the organization.

References

 https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question ??

The End