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

Dr. Laxmidhar Biswal

January 27, 2025

Compare and contrast various types of security controls

Introduction/Motivation

In the last semester, we delved into the fascinating realm of Computer Networking: Concepts, exploring the core of modern communication and information systems. We learned how devices like computers, routers, and servers establish seamless communication. Key principles such as IP addressing, routing, switching, and network topology were emphasized, providing clarity on the backbone of networking. Cisco Packet Tracer emerged as a vital tool, empowering users to design virtual networks, configure devices, and resolve connectivity challenges in a controlled, simulated environment. Its intuitive interface enriched our learning of core networking concepts such as VLANs, OSPF, and NAT, bridging theoretical knowledge with hands-on proficiency vital for real-world network management.

Introduction/Motivation

As networks grow, safeguarding against breaches, malware, and unauthorized access is crucial for managing digital information resources. Understanding firewalls, encryption, and secure protocols ensures confidentiality, integrity, and availability, empowering professionals to design resilient systems and defend against evolving cyberattacks effectively. So, we are going to study computer networking security to protect critical systems, data, and communications from cyber threats.
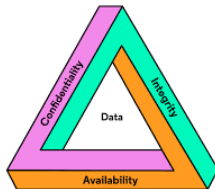
Key security concepts and practices

In the field of Computer Networking, security encompasses the methodologies, tools, and personnel employed to safeguard an organization's digital resources. In essence, security refers to the systematic practice of defending systems, networks, and data against malicious threats, unauthorized access, and potential damage.

CIA Triad

CIA stands as "Confidentiality", "Integrity", "Availability", and Triad means "a group of closely connected."
CIA Triad represents the fundamental principle essential for the protection of systems, networks, and data within the domain of information security.

Key security concepts and practices

Types of security controls

1. Preventative: measures implemented before a threat
2. Deterrent: to warn/discourage a would-be intruducator.
3. Detective: to identify and react to security incidents promptly.
4. Correcting: measures taken to repair damage or restore resources.
5. Compensating: providing an alternative measure to satisfy security requirements when primary controls are not feasible or effective.
6. Directive: mandatory compliance with policies and guidelines to manage security risks.

Key security concepts and practices

Different Level of security controls

1. Technical
2. Manegerial
3. Operational
4. Physical

Technical Controls

- minimization vulnerabilities such as; computer networks, software, and data management.
- Example of effective technical control measures:
  - Firewalls: Oversee incoming and outgoing network traffic, implement filtering mechanisms to identify and block potential threats, and mitigate the risk of unauthorized intrusions.

Key security concepts and practices

Technical Controls.....

- Data encryption: transforms sensitive information into an encoded format, rendering it unreadable to unauthorized parties. Without the decryption key, the information remains secure and inaccessible which mitigates the risk of data breaches.

Managerial Controls

Also referred to as administrative controls, these encompass policies, procedures, and guidelines designed to oversee and manage information systems. Examples include security training programs, contingency planning, and risk assessment.

Key security concepts and practices

Operational Controls

It focuses on executing daily activities and processes essential for delivering goods and services. They involve managing procedures, ensuring quality compliance, improving productivity, and optimizing efficiency. These policies are implemented by personnel who are vital to maintaining smooth operations and maximizing output, thereby enhancing organizational performance and achieving objectives. Example of Operation controls:

- Incident response procedures
- Security awareness training
- User access management

Key security concepts and practices

Physical Controls

Physical controls are essential to overall security, focusing on safeguarding an organization's tangible assets, facilities, and resources. These controls implement measures to prevent unauthorized access, ensure safety, and mitigate physical security risks. A key component includes access control systems that regulate entry to restricted areas, using mechanisms like key cards, biometrics, or PINs. Examples of physical controls:

- Access control vestibule: An access control vestibule is a secured, two-door buffer zone requiring multi-factor authentication for entry into restricted areas.
- Biometric locks: Biometric locks verify identity using fingerprints, iris patterns, or facial recognition for secure access.

Key security concepts and practices

Physical Controls

- **Guards/security personnel:** Guards serve as visible deterrents, ensuring security through monitoring, patrolling, and enforcing protocols.

- **Security fences:** Security fences with metal or wire deter unauthorized access, often enhanced with barbed wire or electricity.

- **CCTV surveillance systems:** Surveillance systems, strategically placed, monitor key areas like entry points and parking lots, aiding in threat detection and incident investigation.

- **Mantraps:** Mantraps are secure enclosures with two interlocking doors, allowing one person at a time to ensure authorized access.

Key security concepts and practices

Physical Controls

- Vehicle barriers: Physical controls like bollards, gates, tire spikes, and hydraulic barriers are used to restrict unauthorized vehicle access to areas.

- Tamper-evident seals: Tamper-evident seals are designed to show visible signs of tampering, such as color changes or broken seals, indicating unauthorized access.

Key security concepts and practices

References

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

Question
??

The End