FORESEC

Guide to Network Security Fundamentals

C

Chapter 1

FORESEC

Learning Objectives

- Understand network security
- Understand security threat trends and their ramifications
- Understand the goals of network security
- Determine the factors involved in a secure network strategy

Understanding Network Security

- Network security
  - Process by which digital information assets are protected
- Goals
  - Maintain integrity
  - Protect confidentiality
  - Assure availability

Understanding Network Security

- Security ensures that users:
  - Perform only tasks they are authorized to do
  - Obtain only information they are authorized to have
  - Cannot cause damage to data, applications, or operating environment

Security Threats

- Identity theft
- Privacy concerns
- Wireless access

To Offset Security Threats

- Integrity
  - Assurance that data is not altered or destroyed in an unauthorized manner
- Confidentiality
  - Protection of data from unauthorized disclosure to a third party
- Availability
  - Continuous operation of computing systems

FORESEC

Security Ramifications: Costs of Intrusion

- Causes of network security threats
  - Technology weaknesses
  - Configuration weaknesses
  - Policy weaknesses
  - Human error

Technology Weaknesses

- TCP/IP
- Operating systems
- Network equipment

Configuration Weaknesses

- Unsecured accounts
- System accounts with easily guessed passwords
- Misconfigured Internet services
- Unsecured default settings
- Misconfigured network equipment
- Trojan horse programs
- Vandals
- Viruses

Policy Weaknesses

- Lack of a written security policy
- Politics
- High turnover
- Concise access controls not applied
- Software and hardware installation and changes do not follow policy
- Proper security
- Nonexistent disaster recovery plan

Human Error

- Accident
- Ignorance
- Workload
- Dishonesty
- Impersonation
- Disgruntled employees
- Snoops
- Denial-of-service attacks

Goals of Network Security

- Achieve the state where any action that is not expressly permitted is prohibited
  - Eliminate theft
  - Determine authentication
  - Identify assumptions
  - Control secrets

Creating a Secure Network Strategy

- Address both internal and external threats
- Define policies and procedures
- Reduce risk across across perimeter security, the Internet, intranets, and LANs

FORESEC

Creating a Secure Network Strategy

- Human factors
- Know your weaknesses
- Limit access
- Achieve security through persistence
  - Develop change management process
- Remember physical security
- Perimeter security
  - Control access to critical network applications, data, and services

continued…

Creating a Secure Network Strategy

- Firewalls
  - Prevent unauthorized access to or from private network
  - Create protective layer between network and outside world
  - Replicate network at point of entry in order to receive and transmit authorized data
  - Have built-in filters
  - Log attempted intrusions and create reports

continued…

Creating a Secure Network Strategy

- Web and file servers
- Access control
  - Ensures that only legitimate traffic is allowed into or out of the network
    - Passwords
    - PINs
    - Smartcards

Creating a Secure Network Strategy

- Change management
  - Document changes to *all* areas of IT infrastructure
- Encryption
  - Ensures messages cannot be intercepted or read by anyone other than the intended person(s)

FORRESTER

continued…

Creating a Secure Network Strategy

- Intrusion detection system (IDS)
  - Provides 24/7 network surveillance
  - Analyzes packet data streams within the network
  - Searches for unauthorized activity

Chapter Summary

- Understanding network security
- Security threats
- Security ramifications
- Goals of network security
- Creating a secure network strategy