Security Policy

TOPICS

- Objectives
- WLAN Security Policy
- General Security Policy
- Functional Security Policy
- Conclusion

Objectives

- Learn the different phases of security policy development
- Understand the purpose and goals of different security policies.

WLAN Security Policy

- Wireless LAN Security Policy falls into two categories:
  - General Security Policy
  - Functional Security Policy

General Security Policy

- General Security Policy consists of:
  - Getting Started
  - Risk Assessment
  - Impact Analysis
  - Security Auditing

Getting Started

- Every Organization with wireless technology needs a policy in accordance with a security plan.
  - Statement of authority

    Emergency Response Team

    Applicable Audience

    Violation reporting procedures and Enforcement

- This plan should address at least the following three issues:
  - Resources – Controlled access to prevent unauthorized users from consuming limited wireless network resources.
  - Privacy - controlled access to prevent unauthorized users from accessing confidential or sensitive data located on the network.
  - Intrusion Monitoring – a monitored environment alerts an organization about unauthorized activities and allows security managers to respond appropriately. (Emergency Resource Team) & (IT security/admin team)

Risk Assessment

- Risk Assessment:
  - Risk Assessment is the process of examining each scenario in which an organization can experience loss due to negative impact events.
  - Risk Assessment involves four themes that require analysis prior to creating a security policy. These include:
    - Asset protection (sensitive data, network services)
    - Threat Prevention
    - Legal liabilities
    - Costs

Impact Analysis

- Impact Analysis help organizations understand the degree of potential and associated loss that could be involved with a network intrusion.

- It covers not only direct financial loss but many other issues such as loss of customer confidence, reputation damage, regulatory effects etc.

Security Auditing

- Wireless security audits identify flaws in wireless networks before the networks become exposed to a malicious threat.

- It recommends organizations periodically engage in security reviews involving independent consultants.

  - Internal Testing
  - Independent Testing
  - Sources of Information

Functional Policy: Guidelines & Baselines

- Every Security policy, at a minimum ,should cover topics that include:
  - Policy Change, Control & Review
  - Password Policies
  - Networking staff and user training requirements
  - Acceptable use
  - Consistent implementation
  - Readily available implementation and management procedures
  - Regular audits and penetration tests by independent professionals.

Password Polices

- Choosing a strong password
  - What to do:
    - Use a password that is mixed case and uses alpha and numeric digits
    - Force periodic password changes through network security mechanisms
    - Lockout accounts after 5 unsuccessful login attempts
    - Make sure all passwords are at least 8 characters in length and use other forms of authentication such as ***smart cards*** or ***biometrics*** in combination with passwords when users need more secure levels of authentication

Cont..

- What not to do:
  - Use a user name, first name or last name.
  - Use pet’s name, child’s name or spouse’s name.
  - Use of number combination such as telephone numbers, social security, birth dates or home address numbers.
  - Use of a common word found in the dictionary
  - Allow passwords to be reused

Networking staff and user training requirements

- The needed training for network staff will include:
  - Wireless hardware implementation, configuration and maintenance.
  - Wireless software: protocol analyzers, intrusion detection systems, configuration management etc.
  - Wireless standards and certifications.

Cont…

- The training needed by end users will include:
  - Acceptable use training: Networking Staff, Contractors, Visitors, Consultants

    Violation Enforcement
    - Who can use the wireless connections?
    - For what purpose may they be used?
    - What purposes are banned from wireless use?
  - Connecting to the wireless network.
    - Understand data rate issues.
    - Distance from the access point.
    - Number of users connected.

Acceptable use

- Acceptable use polices are used to outline the proper use of computer systems and network services available in an organization.
- In order to prevent the introduction of viruses, worms, spyware and other malicious software, the policy should outline how a user must interact with these systems.
- An acceptable use policy should include:
  - Allowed actions.
  - Disallowed actions.
  - Personal use rules.

Baseline Practices

- Baseline practices should be consider the minimum security.
- It will eliminate 95% of all the wireless LAN security.
- A thorough list include:
  - WPA or WPA2 must be used in place of WEP.
  - Default passwords are always weak passwords.
  - Default configuration setting on all access points should be changed.
  - **SSID**: Default SSID should be changed on all access points.
  - **MAC Filters**:
    - MAC filters should not be relied upon to prevent unauthorized access to the WLAN.
    - MAC address filtering is another method by which the IEEE 802.11 task group attempted to secure wireless network.

Cont…

- **Firmware Upgrades:**
  - Periodic firmware upgrades can provide new security functionality and compatibility.
  - Firmware should be upgraded as necessary for the following devices:
    - Access Points
    - Wireless Bridges
    - Client Devices
    - Enterprise Wireless Gateways
    - Enterprise Encryption Gateways.
  - Firmware upgrades are suggested ASAP in order to gain any of the following features:
    - TKIP support (legacy) – WPA/WPA2 uses CCMP
    - Kerberos support
    - 802.1x/EAP support
    - WPA compliance
    - AES support
    - VPN support
    - Rogue access point detection
    - RADIUS or LDAP support (AAA will discuss in future sessions)
    - Role-based access control (RBAC instead of MAC) – discussed later

Functional Policy Monitoring and Responses

- **Rogue Equipment**:
  - The process of eliminating rogue devices include:
    - Setting Corporate Policy Regarding Rogue Equipment
    - Network Administrator Training
    - Help Desk & End User Training
    - Intrusion Detection Systems & Audits.
- **SNMP Community Strings**: It should be changed or disabled.
- **Discovery Protocols:** When discovery protocols are not in use, they should be disabled.

Functional Policy: Design & Implementation

- The Design and Implementation section of the Functional Policy include:
  - Interoperability
  - Layering
  - Segmentation and VLANs
  - Authentication
  - Encryption

Interoperability

- Interoperability is the capability of different mechanisms or network processes from differing vendors to communicate.
- By including interoperability as a policy statement, one ensure that only widely compatible equipment and solutions are implemented.

Layering

- Layering solutions is a method of utilizing solutions from different layers of the OSI model.
- It can provide very high levels of security, but it may also introduce a significant amount of complexity to the implementation and administration of the network.
- The four components to be addressed when layering is considered are:
  - OSI Layer of each solution considered
  - Costs versus benefits
  - Management resources required
  - Throughput & Latency.

Segmentation & VLANs

- Segmentation is a method of implementing solutions that divide the network into smaller, more manageable pieces by using controlled layer 2 and layer 3 boundaries.
- Wired VLANs may be used in place where the physical separation of the wireless network is not possible.

Authentication & Encryption

- Authentication & Encryption help alleviate security risks involved in implementing wireless solutions
- They assist in determining who can access the network and determine whether the data is encrypted while it traverses the wireless segment.
- The choice of what type of authentication and encryption to use for the deployment of a secure WLAN will include the consideration of :
  - Existing implementations
  - Data Sensitivity
  - Scalability (ability of a system, network, or process, to handle growing amounts of work without diminishing QoS)
  - Availability
  - Budget

Conclusion

- Each organization needs to evaluate and design policies, procedures and training tailored to the unique conditions found in their environment.
- Physical security is always an important component of a good policy.
- Audits should be considered to identify where further training is needed and to measure the effectiveness of current policies.