Aplicación de mecanismos de seguridad activa

Objetivos

Los objetivos de esta sección sobre la aplicación de mecanismos de seguridad activa son:

1. Comprender los sistemas de identificación digital.
2. Conocer los métodos de control de acceso.
3. Analizar la función de los cortafuegos en la protección de equipos y servidores.
4. Aprender a seleccionar y configurar cortafuegos de manera efectiva.

Mapa conceptual

- **Sistemas de identificación digital**:
    - **Identificación y autenticación**
    - **Firma electrónica y certificado digital**

- **Control de acceso**:
    - **Listas de control de acceso**
    - **Política de contraseñas**

- **Cortafuegos en equipos y servidores**:
    - **Cortafuegos físico (hardware firewall)**
    - **Cortafuegos lógico (software firewall)**
    - **Selección del cortafuegos**
    - **Configuración del cortafuegos**

Glosario

- **Seguridad activa**: Conjunto de medidas y herramientas que actúan para prevenir, detectar y responder a amenazas en tiempo real.
- **Identificación digital**: Proceso de verificar la identidad de un usuario mediante credenciales digitales.
- **Firma electrónica**: Método de autenticar la identidad de un firmante y garantizar la integridad de un documento digital.
- **Certificado digital**: Documento electrónico que certifica la identidad de una persona o entidad y permite realizar transacciones seguras.
- **Control de acceso**: Conjunto de políticas y mecanismos que regulan el acceso a recursos y sistemas.
- **Cortafuegos (firewall)**: Sistema de seguridad que controla y filtra el tráfico de red para prevenir accesos no autorizados.

5.1. Introducción

Los mecanismos de seguridad activa son esenciales para proteger los sistemas y datos frente a amenazas y ataques. Estos mecanismos incluyen tecnologías y procedimientos que actúan de forma proactiva para prevenir, detectar y responder a incidentes de seguridad.

5.2. Sistemas de identificación digital

Los sistemas de identificación digital permiten verificar la identidad de los usuarios y garantizar la autenticidad de las transacciones y comunicaciones electrónicas.

5.2.1. Identificación y autenticación

- **Identificación**: Proceso mediante el cual un usuario proporciona una identidad única, como un nombre de usuario.
- **Autenticación**: Proceso de verificar que la identidad proporcionada corresponde al usuario, mediante contraseñas, biometría, tarjetas inteligentes, etc.
    - **Métodos de autenticación**:
        - **Autenticación de un solo factor (SFA)**: Uso de una única credencial, como una contraseña.
        - **Autenticación de dos factores (2FA)**: Uso de dos credenciales diferentes, como una contraseña y un código enviado al móvil.
        - **Autenticación multifactor (MFA)**: Uso de múltiples credenciales, como una contraseña, una huella digital y un token de seguridad.

5.2.2. Firma electrónica y certificado digital

- **Firma electrónica**: Proceso que permite la identificación del firmante y garantiza la integridad del documento firmado electrónicamente.
    - **Tipos de firma electrónica**:
        - **Firma electrónica simple**: Incluye métodos básicos como un nombre escrito al final de un correo electrónico.
        - **Firma electrónica avanzada**: Garantiza la vinculación única al firmante y permite su identificación.

        - **Firma electrónica cualificada**: Equivalente a una firma manuscrita, respaldada por un certificado cualificado.

- **Certificado digital**: Documento electrónico emitido por una autoridad de certificación (CA) que verifica la identidad del titular y permite realizar transacciones seguras.
    - **Componentes del certificado digital**:
        - **Clave pública**: Utilizada para cifrar y verificar firmas digitales.
        - **Clave privada**: Utilizada para descifrar y crear firmas digitales.
        - **Autoridad de certificación (CA)**: Entidad que emite y gestiona los certificados digitales.

5.3. Control de acceso

El control de acceso es fundamental para garantizar que solo las personas autorizadas puedan acceder a los recursos y sistemas.

5.3.1. Listas de control de acceso

- **ACL (Access Control List)**: Listas que definen qué usuarios o sistemas tienen permiso para acceder a determinados recursos y qué tipo de operaciones pueden realizar.
    - **Tipos de ACL**:
        - **ACL estándar**: Permiten o deniegan el acceso basado en direcciones IP.

        - **ACL extendida**: Permiten o deniegan el acceso basado en múltiples criterios, como direcciones IP, puertos, y protocolos.

- **Implementación de ACL**:
    - **Definición de reglas**: Establecimiento de políticas de acceso específicas.
    - **Monitoreo y revisión**: Supervisión continua y actualización de las listas de control de acceso.

5.3.2. Política de contraseñas

- **Definición de políticas**: Establecimiento de normas para la creación y gestión de contraseñas seguras.
    - **Requisitos de complejidad**: Incluir letras mayúsculas, minúsculas, números y caracteres especiales.
    - **Longitud mínima**: Establecer una longitud mínima de caracteres para las contraseñas.
    - **Frecuencia de cambio**: Requerir cambios periódicos de contraseña para reducir el riesgo de compromiso.
    - **Manejo de contraseñas**: Utilizar herramientas y prácticas seguras para almacenar y gestionar contraseñas, como gestores de contraseñas y políticas de no reutilización.

5.4. Cortafuegos en equipos y servidores

Los cortafuegos son una línea de defensa crucial para proteger los sistemas contra accesos no autorizados y ataques.

5.4.1. Cortafuegos físico (hardware firewall)

- **Descripción**: Dispositivos físicos dedicados que filtran el tráfico de red entre la red interna y externa.
- **Características**: Ofrecen mayor rendimiento y seguridad, y son ideales para entornos empresariales.

5.4.2. Cortafuegos lógico (software firewall)

- **Descripción**: Programas instalados en servidores o equipos individuales que controlan el tráfico de red entrante y saliente.
- **Características**: Flexibilidad y facilidad de actualización, adecuados para uso individual o en pequeñas redes.

5.4.3. Selección del cortafuegos

- **Evaluación de necesidades**: Considerar el tamaño de la red, el volumen de tráfico y los requisitos de seguridad.
- **Comparación de opciones**: Analizar las características, costos y beneficios de diferentes soluciones de cortafuegos.

5.4.4. Configuración del cortafuegos

- **Definición de reglas**: Establecer políticas de acceso que determinen qué tráfico se permite y cuál se bloquea.
- **Monitoreo y ajustes**: Supervisar el rendimiento del cortafuegos y ajustar las configuraciones según sea necesario para responder a nuevas amenazas.