SEGURIDAD LOGICA

Identificación y Autentificación

Primera línea de defensa que previene el ingreso de usuarios no autorizados.

- Identificación: momento en que el usuario se da a conocer en el sistema.
- Autenticación: Verificación que realiza el sistema sobre esa identificación.

Distintos métodos de autenticación de manera física:

1. Algo que solamente el individuo conoce: palabra clave, pin, etc.
2. Algo que la persona posee: tarjeta magnética
3. Algo que el individuo es y lo identifica: huellas digitales
4. Algo que el individuo es capaz de hacer: patrones de escritura

Idealmente se busca que el usuario se identifique una sola vez en el sistema y que pueda realizar todas las operaciones. Esto se denomina “single login”. Para poder realizar esto, es conveniente contar con un servidor de autenticaciones.

La seguridad informática se basa en la efectiva administración de los permisos de acceso de usuarios. Esta administración abarca:

- Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios.
- Identificación de los usuarios con norma homogénea para toda la organización.
- Revisión periódica sobre la administración de las cuentas y los permisos de acceso establecidos.
- Revisiones orientadas a verificar la adecuación de los permisos de acceso de cada individuo.
- Detección de actividades no autorizadas.
- Consideraciones relacionadas con cambios en la asignación de funciones del empleado.
- Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización.

Modalidad de Acceso

Hace referencia al modo de acceso que se permite sobre los recursos y la información. Puede ser:

- **Lectura**: El usuario solamente puede leer o visualizar la información.
- **Escritura**: Permite agregar datos, modificar o borrar información.
- **Ejecución**: Ejecuta programas.
- **Borrado**: Permite borrar y/o eliminar recursos del sistema.
- **Todas las anteriores**
- **Creación:** Permite crear nuevos archivos, registros, etc.
- **Búsqueda:** Permite listar los archivos de un directorio.

Control de Acceso Interno

Se utiliza para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Es un método poco seguro.

- **Sincronización de passwords:** consiste en que un usuario tenga acceso a diferentes sistemas interrelacionados con la misma password. Para implementar dicha sincronización, todos los sistemas deben tener un alto nivel de seguridad.
- **Caducidad y control:** controla cuando pueden/deben cambiar sus passwords los usuarios. Se define un periodo de tiempo.

Cifrado

El cifrado de datos puede proveer una potente medida de control de acceso. Dicha información solo puede ser descifrada por el usuario que posea la clave apropiada.

Lista de Control de Accesos

Varían en su capacidad y flexibilidad, son aquellas que se refieren a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema.

Limites sobre la Interfaz de Usuario

Se suelen utilizar junto con las listas anteriormente mencionadas para restringir a los usuarios a funciones específicas.

Etiquetas de Seguridad

Designaciones otorgadas a los recursos que pueden utilizarse para varios propósitos, por ejemplo, control de accesos.

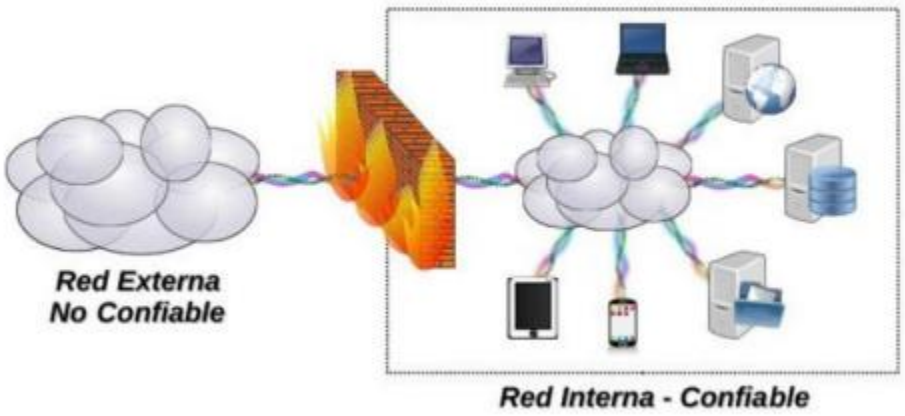
Control de Acceso Externo

Dispositivos de Control de Puertos

Dispositivos que autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo.

Firewalls o Puertas de Seguridad

Dispositivo de red que crea una separación entre redes publicas y privadas mediante el análisis de trafico de red permitiendo solamente el paso de cierto trafico entre la red no confiable y la red confiable.



Características Básicas

- Dispositivos de defensa perimetral que separan redes
- Filtrar el tráfico dependiendo reglas predefinidas
- No protegen de ataques internos
- No protegen de accesos no autorizados
- No protegen de la totalidad de ataques dañinos

Clasificación de Firewalls

- **Tipo Software:** Son componentes lógicos que funcionan en una computadora.
- **Dispositivos de Hardware:** Han sido diseñados para cumplir esta tarea especifica.

Funcionalidades Accesorias

Por ubicación estratégica en la arquitectura de la red, suelen incorporar otras funcionalidades de alcance perimetral a fin de agregar valor al producto.

Defensa en Profundidad

Por medio del uso de múltiples tipos de firewalls en serie, se puede obtener los beneficios de todos y no ser vulnerable a la debilidad de uno solo.

DMZ – Zona Desmilitarizada

Área de configuración del firewall con reglas especificas orientada a manejar equipos que deben tener mayor exposición en la infraestructura.

Tipos de Firewall

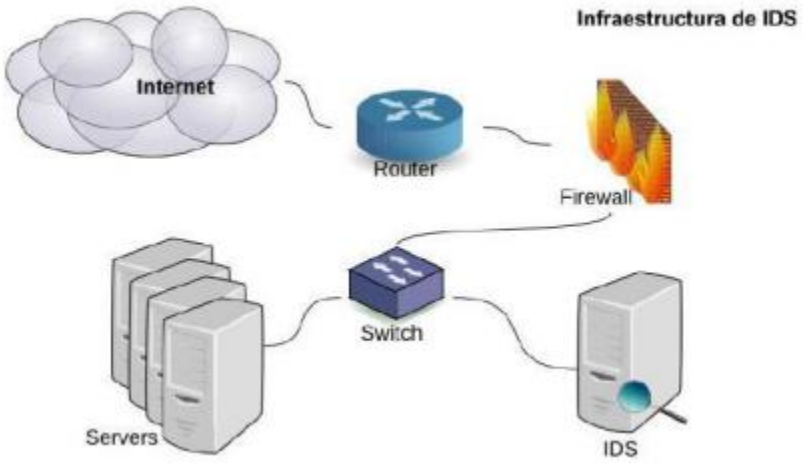
- **Packet Filters:** Monitorea las direcciones de IP de origen y destino, verificando puertos, pero no el contenido de la comunicación. Ejerce nivel 3 del modelo TCP/IP.
- **Circuit Level Gateways:** Opera en la capa TCP permitiendo conexiones a través de el y creando un circuito para monitorear la conexión con una verificación de contenido limitada.
- **Application Level Gateways:** Conocidos como proxies, al igual que los anteriores, pero estos son específicos para cada aplicación.
- **State-Full Multilayer Inspection:** Combina los 3 anteriores, usa protocolos de control de paso de contenidos a través de reglas de validación.

Firewalls Personales

Dispositivos lógicos que se instalan en la propia terminal y permiten aplicar filtros a la información de red correspondiente a cada interfaz y/o aplicación.

IDS – Sistema de Detección de Intrusiones

Elemento que detecta, identifica y responde a actividades no autorizadas o anormales.



Modelo de Funcionamiento General

1. **Recolección de datos:** Registro de auditorías, sistemas, aplicaciones, etc.
2. **Análisis:** Análisis de usos indebidos, anomalías.
3. **Respuesta:** Activa o Pasiva.

Clasificaciones de IDS

1. **Fuente de datos**

- **HIDS:** Utilizan los registros de auditoría, registros del sistema, etc.
- **NIDS y NNIDS:** Utilizan paquetes de red (TCP, IP, etc.) con posibilidad de utilizar agentes (IDS)

2. **Metodología de análisis**

- **Detección de uso indebido**
- **Detección de anomalías**

3. **Modo de Respuesta**

- **Respuesta Pasiva:** Genera una alerta
- **Respuesta Activa:** Toma una acción automática para evitar la continuidad

IPS – Sistemas de Prevención de Intrusiones

Combinación entre IDS + Firewall en respuesta activa. Identifican el curso de ataque y lo bloquean.

Dispositivos UTM

Firewalls de red que manejan diferentes servicios en un mismo equipo.

- Función VPN
- Antispam
- Antiphishing
- Antispyware
- Filtrado de contenidos
- Antivirus de perímetro
- Detección/Prevención de Intrusos (IDS/IPS)

Funcionan en forma de sistemas de control de acceso a redes. Se pueden integrar con toda la infraestructura legacy utilizando SOA (Service Oriented Architecture) y otras arquitecturas extensibles.

- **Modo Proxy:** Uso de proxies para procesar y redirigir todo el trafico interno.
- **Modo Transparente:** No redirigen, solo procesan y son capaces de analizar el paquete en tiempo real.

NGFW – Next Generation Firewalls

Se basa en la inspección profunda de paquetes, sumada a las tecnologías para evitar intrusiones. Se busca la combinación de las distintas capacidades de firewalls a nivel de la red con inspección profunda en paquetes y pueda incorporar nuevas características para resolver nuevas amenazas.

WAF – Web Application Firewall

Dispositivo físico o lógico que analiza el trafico web, los datos recibidos por parte del usuario y protege de diferentes ataques web.

- **Modelo de Seguridad Positiva:** Por medio de una serie de reglas definidas, deniegan por defecto todas las transacciones y solamente acepta las que identifica como seguras o validas. Difícil de mantener. No dependen de actualizaciones
- **Modelo de Seguridad Negativa:** Acepta todas las transacciones y deniega aquellas que detecta como amenaza o ataque.

Es común que puedan detectar un posible buffer overflow analizando las variables que entran por GET y POST. Para los ataques Cross Site Scripting y SQL injection, vigila los valores pasados por GET y POST nuevamente y bloquea valores que contengan SELECT FROM, UNION, etc.

Analiza también la respuesta del servidor, si una petición tiene como respuesta una cuenta bancaria, por ejemplo, niega dicha respuesta por parte del servidor.

Riesgos de un WAF

Si no están configurados correctamente, pueden detectar falsos positivos. Necesitan adaptación y configuración ante nuevos cambios en el funcionamiento de la aplicación. Pueden también, producir retardos en las operaciones. Para ello, se implementan aceleradores SSL.

Modos de Funcionamiento

Pueden funcionar en modo bridge, router, proxy o plugin. Pueden ser hardware o software. Pueden denegar peticiones provenientes de ciertos puntos geográficos.

Administración y Seguridad

Administración del Personal y Usuarios – Organización del Personal

- **Definición de Puestos:** Otorgar el mínimo permiso de acceso requerido a cada puesto de trabajo.
- **Determinación de la Sensibilidad del Puesto:** Determinar si la función requiere permisos riesgosos que le permitan alterar procesos.
- **Elección de la Perona para cada Puesto:** Considerar experiencia y conocimientos técnicos.
- **Entrenamiento Inicial y Continuo**

Estas capacitaciones son esenciales para todo el personal y solamente una vez que estén totalmente capacitados y posean la conciencia respecto de la seguridad, podrán asumir las responsabilidades individuales.

Seguridad Física

Puede deberse a distintos factores:

Incendios

Una de las principales causas de este inconveniente es la falla de instalaciones eléctricas defectuosas, el inadecuado almacenamiento y traslado de sustancias peligrosas, etc.

Es importante la seguridad en los centros de cómputos y para ello, estos deben estar instalados solamente en áreas donde el personal este autorizado a ingresar únicamente. Deben contar con equipos de ventilación y detección de incendios.

Condiciones Climatológicas

Debe tenerse en cuenta a la hora de la construcción de un edificio, la frecuencia y la severidad de la ocurrencia de distintos eventos climatológicos, tales como terremotos, tifones, etc.

Instalación Eléctrica

Tener en cuenta los picos y ruidos electromagnéticos, es decir las subidas y bajadas de tensión. Mismo el ruido que interfiere en el funcionamiento de los componentes electrónicos. A tener en cuenta:

- Cableado de alto nivel
- Pisos de Placas Extraíbles
- Sistema de Aire Acondicionado
- Emisiones Electromagnéticas

Ergometría

Enfoque que plantea la adaptación de los métodos, los objetos, las maquinarias, etc. Su fin es la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas, etc.

- Trastornos Óseos y/o musculares
- Trastornos Visuales
- Salud Mental
- Ambiente Luminoso
- Ambiente Climático

Guardia

Control de acceso de todas las personas al edificio ubicados en lugares estratégicos.

- Control de Vehículos

Sistemas Biométricos

Tecnología empleada para el control por medio de mediciones electrónicas. Guarda y compara las características únicas de cada persona.

- Emisión de calor
- Huella Digital
- Verificación de Voz
- Verificación de Patrones Oculares

Protección Electrónica

Es la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas.

- Barreras Infrarrojas
- Detector Ultrasónico
- Detectores Pasivos Sin Alimentación
- Sonorización y Dispositivos Luminosos
- Circuitos Cerrados de Televisión
- Edificios Inteligentes