Síntesis conceptual

Grado: Administración de Sistemas Informáticos en Red
Asignatura: Seguridad y alta disponibilidad
Unidad: 1. Introducción a la seguridad informática

Resumen

Podemos encontrar diversas tipologías de medidas, entre las que destacan:

- Las medidas activas y pasivas.
- Las medidas preventivas y correctivas.

En cuanto a las amenazas estas son múltiples y variadas:

- Desgracias.
- Situaciones de riesgo de *hardware*.
- Averías o fin de la vida útil.
- Robos.
- Accesos no autorizados.
- Accesos ilegítimos.
- *Software* maliciosos.
- Suplantación de identidad.

Elementos de seguridad física y ambiental:

- Ubicación y protección de equipos y servidores: Con el fin de evitar problemas estructurales o de climatización.
- Protección ante fallos del cableado: Cuanto mayor sea el número de equipos mayor será el cableado y, por tanto, los problemas que este puede ocasionar.
- Protección ante humedades e inundaciones: El rango de humedad ideal estaría entre un 45-55% de humedad y se aconseja un doble suelo en caso de inundación.
- Protección ante incendios y altas temperaturas: sala refrigerada y medidas antiincendios.
- Protección ante terremotos: Empleo de estructuras antisísmicas.
- Protección ante problemas de suministro eléctrico: Empleo adecuado de SAI.
- Protección ante accesos no autorizados y robos: Vigilancia y candados antirrobo.

A pesar de todas nuestras preocupaciones se recomienda la contratación de análisis forenses o auditorías que pongan a prueba nuestras defensas.

Las fases de un ataque son las siguientes: reconocimiento, escaneo, obtención de acceso, mantenimiento de acceso y borrado de huellas.

El primero de los mecanismos de seguridad activa es la autentificación, que consiste en, con credenciales, identificarse con el fin de obtener los permisos que poseemos. Cualquier persona no identificada no obtendrá ningún permiso.

El proceso de identificación es llamado acceso o login, este se realiza generalmente mediante el empleo de usuario y contraseña. Con el fin de mantener la seguridad de esta se recomienda

que estas contraseñas se creen empleando ciertos pasos, con el fin de que no sean fáciles de descifrar, como, tener un número mínimo de caracteres, emplear, mayúsculas y minúsculas, etc. También podemos encontrar las contraseñas basadas en patrones o imágenes.
Se emplea también la autentificación en dos pasos, donde tras colocar la contraseña deberemos ratificar la entrada desde nuestro móvil, de modo que la contraseña por sí misma es inútil.

Una vez identificado será la ACL, listas de control de acceso, la que nos de los accesos y permisos que nos corresponden, esta designación se realiza asignando a los usuarios en diferentes grupos, los cuales contendrán los permisos incorporados es posible que un usuario se encuentre en diversos grupos, obteniendo así los permisos de todos ellos.

El empleo de la autentificación es especialmente relevante en sistemas centralizados, donde los datos se comparten. En algunos casos como ocurre con las cuentas de Google, tan solo es necesario identificarse una vez para acceder a diversos elementos, a este concepto se le conoce como Single Sign-On.

Las unidades de almacenamiento poseen algunas propiedades como son:

- Productividad: tiempo de acceso, tasa de transferencia y durabilidad.
- Disponibilidad: acceso a los datos en todo momento.
- Accesibilidad: Control de permiso de acceso.

Podemos crear imágenes de respaldo y copias de seguridad:

- Imágenes de respaldo: Una copia exacta de un disco o de una partición. Se almacena en un fichero único que, una vez transformada, la veremos con la extensión .iso.
- Virtualización de los servidores: Consiste en instalar un sistema operativo especial, el cual nos permite crear máquinas virtuales.
- Copias de seguridad: Un archivo almacenado en una ubicación y que contiene una copia de los datos elegidos previamente por el usuario. Podemos encontrar diversos tipos:
    - Completa.
    - Diferencial.
    - Incremental.

Conceptos fundamentales

- **CPD, Centro de Proceso de datos**: espacio donde se almacenan los servidores de una gran empresa.

- **Autenticidad**: garantía de la identidad de nuestro interlocutor.

- **Armario rack**: armarios especializados para contener diversos dispositivos muy empleado en los CPD.

- **Firewall**: software o hardware que permite controlar el tráfico de datos, evitando así elementos no deseados.

- **PDU**: Unidad de Distribución de Potencia (Power Distribution Unit). Una PDU es lo que comúnmente conocemos como regleta, se distingue del SAI en que esta no posee batería, las más básicas pueden incluso no poseer protección con fusible.