SEGURIDAD INFORMÁTICA

PILARES BÁSICOS

Ing° Pedro Beltrán Canessa

MENU PRINCIPAL

- ¿Qué es la seguridad?
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - Autenticidad
- ¿Qué queremos proteger?
  - Importancia de los elementos
- ¿De qué nos protegemos?
  - Factores humanos
  - Factores no humanos
- Resumen

¿Qué es la seguridad?

La seguridad está finamente ligada a la certeza. Hay que aclarar que no existe la seguridad absoluta, más bien, lo que se intenta minimizar es el impacto y/o el riesgo. Por tal motivo, cuando hablamos de inseguridad, debemos hacerlo en carácter de niveles, y lo que se intenta y se debe hacer es llevar cabo una organización efectiva a fin de lograr llegar a los niveles más altos.

PILARES BÁSICOS

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad

CONFIDENCIALIDAD

La información puede ser accedida únicamente por las personas que tienen autorización para hacerlo. Por ejemplo, cuando decimos que Internet es una Red de redes, estamos diciendo que hay medios que se entrelazan entre sí para lograr vinculación. Es por ello que la confidencialidad se puede ver amenazada si alguien intercepta los paquetes que viajan de un lado a otro.

INTEGRIDAD

Cuando nos referimos a integridad, queremos decir que estamos totalmente seguros de que la información no ha sido borrada, copiada o alterada, no sólo en su trayecto, sino también en su origen.

DISPONIBILIDAD

Este término hace referencia al método de precaución contra posibles daños, tanto en la información como en el acceso a la misma: ataques, accidentes o, simplemente, descuidos pueden ser los factores que obligan a diseñar métodos para posibles bloqueos.

AUTENTICIDAD

La integridad nos informa que el archivo no ha sido retocado ni editado, y la autenticidad nos informa que el archivo en cuestión es el real.

AUTENTICACIÓN

Para una PC, autenticar no es lo mismo que identificar. Por ejemplo, en un sistema de seguridad donde se verifica la voz, el sistema se encarga de buscar un patrón en su voz para distinguir quién es. Este reconocimiento es de identificación, pero todavía falta la parte en que el usuario dice una frase o palabra clave, y es aquí donde la autenticación tiene efecto.

MÉTODOS DE AUTENTICACIÓN

Categoría 1: algo que el usuario sabe.

Un dato esencial, puede tratarse de algo de su persona o bien de un simple o complejo password (contraseña).

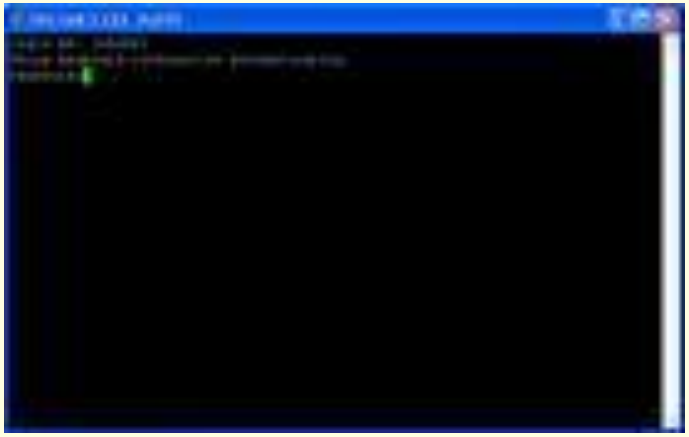

Imagen que nos muestra un sistema de verificación por medio de usuario y password en el sistema operativo Unix.

MÉTODOS DE AUTENTICACIÓN

Categoría 2: algo que el usuario lleva consigo.

Puede ser un documento de identidad, una tarjeta o cualquier otro elemento que uno lleve consigo.

MÉTODOS DE AUTENTICACIÓN

Categoría 3: propiedad física o acto involuntario.

La pupila, la voz y la huella dactilar son ejemplo de propiedades físicas de un individuo y firmar es un acto involuntario, ya que uno no está pensando en hacer cada trazo, sino que los realiza en conjunto.

¿Qué queremos proteger?

Cuando hablamos de seguridad informática muchas veces se confunde diciendo seguridad en Internet. Informática comprende otro contexto, como ser el de seguridad física, mientras que el otro se limita a hablar del entorno que a Internet se refiere. Por tales motivos, la seguridad informática intenta proteger cuatro elementos:

- Hardware
- Software
- Datos
- Elementos fungibles

HARDWARE

Este término hace referencia al método de precaución contra posibles daños, tanto en la información como en el acceso a la misma: ataques, accidentes o, simplemente, descuidos pueden ser los factores que obligan a diseñar métodos para posibles bloqueos.

SOFTWARE

El software consiste en el conjunto de sistemas lógicos que hacen funcional al hardware: sistemas operativos, aplicaciones, programas, etc.

DATOS

Conjunto de sistemas lógicos que tienen como función manejar el software y el hardware (registros, entradas de bases de datos, paquetes que viajan por los cables de red)

ELEMENTOS FUNGIBLES

Son elementos que se gastan con el uso continuo (papel, toner, insumos en general). Algunos administradores de seguridad no consideran estos elementos, pero una buena administración se basa en controlar los recursos de la empresa, ya que los mismos no son infinitos ni el dinero con el que se cuenta es ilimitado. Para lograr eficiencia y calidad se tiene que tomar conciencia y crear una política para el correcto uso de las herramientas con las que cuenta la empresa.

IMPORTANCIA DE LOS ELEMENTOS

Los datos son los principales a la hora de proteger. El hardware, el software y los elementos fungibles son recuperables desde su origen (comprándolos o instalándolos nuevamente), pero los datos no tienen origen, sino que son cambiados con el transcurso del tiempo y son el resultado del trabajo realizado. Ésta es la razón que convierte en muy importante el armado de una política de seguridad consistente en programar horarios para realizar copias de seguridad, archivarlos, tener disponibilidad de espacio/privacidad y, además, poder hallar lo que se necesite en tiempo y forma.

TIPO DE ATAQUES SOBRE LOS DATOS

- Interrupción
- Interceptación
- Fabricación
- Modificación

INTERRUPCIÓN

Ataque contra la disponibilidad.

Cuando los datos o la información de un sistemas se ven corruptos, ya sea porque los mismos se han perdido, se han bloqueado o simplemente porque no están disponibles para su uso.

INTERCEPTACIÓN

Ataque contra la confidencialidad.

Con este tipo de ataque lo que se logra es que un usuario no autorizado pueda tener acceso a un recurso y, por ende, la confidencialidad se vea divulgada .

FABRICACIÓN

Ataque contra la autenticidad.

El ataque contra la autenticidad tiene lugar cuando un usuario malicioso consigue colocar un objeto en el sistema atacado.

Este tipo de ataque puede llevarse a cabo con el objeto de hacer creer que ese archivo/paquete es el correcto o bien con la finalidad de agregar datos y obtener, de esta manera, un provecho propio.

MODIFICACIÓN

Ataque contra la integridad.

Un atacante, que puede contar o no con autorización para ingresar al sistema, manipula los datos de tal manera que la integridad se ve afectada por su accionar.

Cambiar datos de archivos, modificar paquetes, alterar un programa o aplicación son sólo algunos ejemplos de este tipo de ataque que, sin lugar a dudas, es el que reviste mayor grado de peligrosidad.

¿De qué nos protegemos?

Esta pregunta es tan amplia como su respuesta. Hay muchas clasificaciones , pero la mayoría tienen un punto de vista en común: nos protegemos de las personas.

A esta altura de los tiempos suena raro decir que nos cuidamos de nosotros mismos y, más aún sabiendo que los elementos que protegemos son, en su mayoría, cosas creadas por nosotros mismos. El factor más importante que incita a las personas cometer actos contra los cuatro pilares es, sin ninguna duda, el poder. Este poder reside en los datos y en la información.

FACTORES HUMANOS

Al hablar de factores humanos, incluimos al software y/o malware, ya que los mismos fueron ideados y creados por personas. La responsabilidad no puede atribuirse a un programa por más que éste pueda reproducirse, actuar de forma independiente o tomar decisiones pues su génesis es humana.

FACTORES HUMANOS

EL PERSONAL O LOS EX EMPLEADOS

Son los grupos más poderosos y los que más pueden sacar provecho a los datos.

FACTORES HUMANOS

HACKERS, CRACKERS Y LAMERS

Se trata de muchos de los que intentan entrar en los sistemas de manera externa e interna.

FACTORES HUMANOS

LOS CYBERTERRORISTAS

Son personas que atacan con un fin específico: ya sea por ideologías o por puntos de vista. Por ejemplo, pueden atacar páginas que se manifiestan en contra de su religión o directamente dejar inactivo servidores.

FACTORES HUMANOS

PUERTAS TRASERAS

Muchas veces los programadores dejan atajos que son métodos no convencionales para traspasar autenticaciones o restricciones.

FACTORES NO HUMANOS

Las amenazas ambientales, si bien dependiendo de su ubicación geográfica pueden tener más o menos periodicidad catastrófica, no son hechos que ocurran frecuentemente. Pero esto no es motivo suficiente para no considerar la circunstancia de que, si sucede, el daño será severo.

Las catástrofes más comunes son los terremotos, incendios, atentados, tormentas, etc.

RESUMEN

La seguridad informática abarca numerosas posibilidades de medidas y contramedidas, pero los pilares son siempre los mismos. Aquí se explicó la base y se plantearon algunas terminologías y conceptos que hay que saber a la hora de poder armar una organización adecuada. Lo fundamental, más allá de la teoría, es poder tomar conciencia y analizar mentalmente cuáles son las posibilidades antes de que ocurra el ataque. El éxito de un administrador de seguridad es saber el *cómo*, para luego no tener que preguntarse el *porqué*.

REFERENCIAS

- Firtman, Sebastián - Seguridad Informática – MP Ediciones (2011). Buenos Aires.