Autor: Cygog (Cygog@live.com.ar)

Seguridad en los sistemas informáticos

Nota de autor:

No soy bueno para las introducciones así que voy a lo directo, pero antes, una frase "espero que vean el esfuerzo que he dado y lo sepan valorar".

Empezemos:

Muchos de ustedes saben que el uso de Internet es cada ves mas accesible a cualquier persona, lo cual que para empresas, bancos, administración publica, compañía de seguros etc.. crece la inseguridad y estos administradores se sienten expuestos a que los “roben”, (esto no es así, no se debe pero se puede.. ustedes saben que eso es de lammers..) Okk entonces ya se deben imaginar cuanta plata se pierde por año, una estadística es que el 62% de las empresas sufrió algún ataque o robo..(esto sigue crecienDO)

¿Se puede decir que existe un sistema informático seguro?

Yo diría primero tenemos que saber la definición de seguro, para mi seguro es cuando se puede confiar en el, y hace lo que tiene que hacer, la seguridad se basa en la confianza.. ¿Por qué guardamos plata en un banco? Porque pensamos que es seguro y nos dará la plata cuando la pedimos..

Seguridad según Wikipedia:
El término seguridad proviene de la palabra securitas del latín. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

Todos tenemos que definir cuales son nuestros objetivos y a que nivel de seguridad se quiere llegar…
El termino seguridad es muy amplio y comprende distintos aspectos:

#Confiabilidad: La información solo puede ser accedida por aquel que este autorizado…. (yo si pongo de ejemplo un banco, los administradores y yo podríamos acceder a mi cuenta)
#Integridad: La información no puede ser modificada y modificada sin permiso…(si puse 2 billetes de $100 y luego de varios días tengo 4 de $50 tendría la misma plata pero modificada… en distintos billetes)
#Consistencia: Esto trata sobre lo acordado con por ejemplo el banco..
#Disponibilidad: La información tiene que estar cada vez que la preciso (si me quedo sin dinero voy al banco.. pero esta cerrado xDD no podré sacar dinero)
#Control: Consiste en regular el acceso a la información..

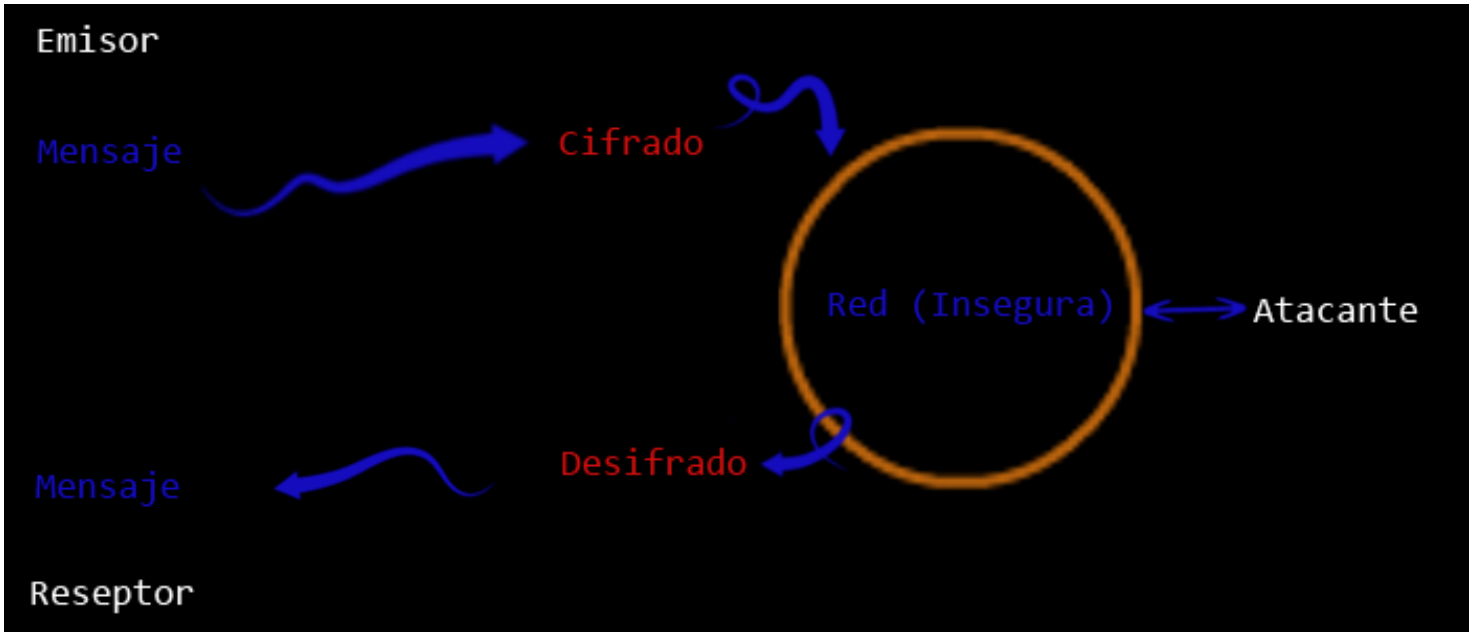
Ustedes pueden determinar en que se enfocaran, su sistema informático, por ejemplo: El banco le dará mas importancia a la integridad y control…
Siempre nos tenemos que preguntar que queremos preservar en nuestro sistema y como… Sabiendo a que peligros nos enfrentamos y que es lo que tenemos que proteger, aumentamos y mejoramos nuestra seguridad en el sistema…
Un factor importante y yo no entrare en detalle de los riegos, unos ejemplos son:

#Virus: Creo que es el mas conocido por todos xD, un virus es un programa malicioso que se propaga por la red y lo único que hace es joder nuestro ordenador..
#Ataques masivos: (los que mas me gustan xD): se ha puesto de moda este ataque que provoca la caída del sistema informático o que quede inutilizado (esto se llama denegación de servicio, o mas conocido como DDOS)

Una vez sepamos cuales son los riesgos, tendríamos que tomar medidas de seguridad, ustedes saben que no pueden ser eliminados, pero, si reducirlos..
Las posible medidas de seguridad que se me ocurren en este momento xD son:
El cifrado de la información, cortafuegos, antivirus, anti-trojanos, etc..

Yo recomiendo la criptografía, el objetivo es asegurar la:
#Confiabilidad: El mensaje no puede ser leído por otra persona.
#Integridad: El mensaje no puede ser modificado por otro individuo
#Autentificación: Se puede verificar si el mensaje ha sido enviado por otra persona y recibido por otra..
Siempre es necesario…
#Proteger la información almacenada en la computadora.
#Proteger la información transmitida hacia otra computadora
No todos los cifrados tienen la misma seguridad ya que algunos pueden tardar dias, meses, años, siglos, en poder descifrar el dato..

Este es un modelo básico.



Hay dos tipos de encriptación: Clave secreta y Cave publica, no entrare en detalle, (jeje tengo sueño)

¿Qué es la seguridad perimetral? Consiste en evitar ataques externos a nuestro sistema informático, la forma mas simple es asegurar nuestro sistema… es no tener ninguna conexión al exterior, pero esto es imposible, ya que la mayoría de los sistemas informáticos necesitan pedir información a otros…

Un firewall (cortafuegos), su función es aislar una determinada zona de problemas externos…la función fundamental es regular la salida y entrada de datos a un sistema.
Les doy un ejemplo, en una pagina de descargas, un firewall determinaría que ficheros pueden descargar, o sea que puede salir del servidor…

Un antivirus, su objetivo es analizar todo el trafico que entra y sale, un antivirus esta en constante actualización, ósea que esta conectado a la base de datos de la empresa fabricadora del software…

Incluso en los sistemas de protección más avanzados, la seguridad perfecta no existe, por lo tanto en este momento podemos tener a nuestra página en la ruina o tener un individuo en nuestro sistema xDD…
Existen varias formas de detectar un intruso, deducir que alguien a entrado porque hay ficheros modificados, hay un comportamiento anormal en la pc…etc. Es muy simple!!

Los dos tipos más importantes de detección de intrusos son los basados en red y los de host.

#Basados en red: Estos detectores son aplicas (ósea aparatos) que están conectados a la red interna de una empresa y analizar el trafico detectando amenazas!!! Algo que aprendí sobre esto es que si el mensaje esta cifrado estos no suelen identificarlo..
#Basados en host: Estos aparatos están instalados en cada computadora de una red…Estos suelen ser mas eficientes pero tienen que ser instalados en todas las computadoras…

Estoy con mucho sueño así que voy a terminar esto…no es raro ver personas trabajando desde su casa, con su portátil, o agendas electrónicas..esto es un arma de doble filo, ya que permite mayor flexibilidad a los empleados y aumentar el riesgo de acceso a la información que se envíen entre estos sistemas..
La solución se llama redes privadas virtuales: El objetivo de esto es que cualquier persona que se conecta remotamente este tan seguro como si estuviera en la empresa. Para esto se utiliza estándares IPSec y EAP.

Espero que les haya gustado. Dudas y proyectos a mi email.
Atte: Cygog