

SEGURIDAD E INTERNET

Hoy en día, mucho se habla sobre computadoras y seguridad en Internet. Mucho de lo cual va exclusivamente dirigido al sector de los negocios y las grandes corporaciones. Mientras éste tipo de discusión y educación es en gran medida requerido, mucha de esta información es de poco uso para nosotros a nivel personal.

Es posible y aún muy probable que una empresa que tenga computadoras, y quizás acceso a Internet tenga su propio administrador o encargado de sistemas. O tenga un contrato con una compañía que esté encargada de dar servicio a sus computadoras o sistemas cuando un problema se presenta. Ese administrador tendrá instaladas todas las últimas actualizaciones de seguridad (patches), y los programas necesarios para mantener fácilmente al negocio libre de riesgos y trabajando.

Pero, muchas veces, ahí es donde nuestra propia protección y seguridad termina. Esto es como tener un guardia en la puerta principal mientras deja la puerta de atrás abierta.

El objetivo principal de cuidar de la seguridad en una red es la de mantener la Disponibilidad, Integridad y Confidencialidad de los recursos.

Disponibilidad

La disponibilidad asegura que los recursos de la red estén operando cuando sean necesarios. Este es el factor más importante debido a que si la Intranet no está operando, no importa que tanta integridad y confidencialidad tenga. Los ataques conocidos como "Negación de Servicio" son orientados a destruir la disponibilidad de una red o de los componentes de esta.

Integridad

La integridad asegura que los datos y los programas están completos, correctos y son auténticos. El objetivo es impedir que personas o programas no autorizados (ej.: virus) hagan cambios en nuestros sistemas y que los usuarios autorizados hagan cambios no autorizados. En las redes se debe asegurar que los mensajes recibidos son los mismos que los enviados para garantizar la integridad. Esto se logra garantizando que los mensajes están completos y sin modificaciones. El mecanismo más común de proteger la integridad es mediante un método que se denomina encriptación y que explicaremos más adelante.

Confidencialidad

El objetivo de la confidencialidad es proteger la información para que no pueda ser vista o copiada por personas no autorizadas. Las herramientas para mantener la confidencialidad son la encriptación y el control de acceso. Este último es el proceso por el cual se limita el privilegio de uso de los recursos de un sistema. Hay tres tipos de controles:

- *Administrativo*: el que se basa exclusivamente en las políticas de una empresa.
- *Físico*: el que se basa en proteger los componentes físicos de los sistemas, como bloquear con llave la puerta de acceso a un centro de cómputos o áreas con contenidos de importancia.
- *Lógico*: es el conjunto de medios usados para limitar el acceso a la información o recursos de manera lógica, como por ejemplo, una clave de acceso al programa de envío de correos electrónicos.

Tomemos como ejemplo el correo electrónico. Millones de "e-mails" son enviados alrededor del mundo diariamente. La gente sufre y escribe sobre sus amores perdidos, esperanzas y sueños. Hablan sobre su condición médica, sobre lo que hizo la noche anterior y sobre los planes que tiene para el fin de semana. Déjeme hacerle una pregunta. ¿Podría usted tomar una postal y enviar un mensaje muy personal a la persona de la cual está enamorada?. Envía en la postal, quizás, ¿el PIN de su cuenta bancaria?. No, seguramente no, pero ¡¡usted está haciendo eso cada vez que envía un correo electrónico!!.

¡Cualquiera que tenga acceso a su computadora podría leer sus e-mails!. Cualquiera que tenga un programa al que comúnmente se llama sniffer (husmeador) podría realizar una exploración de toda la información que entra y sale de su computadora. Su proveedor de Internet, o un empleado de su proveedor, podría ir a su casilla de correo en el servidor de correo y leer sus contenidos. ¿Cree usted que eso no sucede?. Si sucede. Mientras cualquier acceso a su información personal podría ser hecho con la más sana intención. Eso no da menor importancia al hecho de que aún es SU información personal, SU forma de pensar.

¿Cómo se puede proteger usted mismo?. El primer paso es, NUNCA envíe información personal o privada que usted no quiera hacerla pública vía correo electrónico, porque muy bien podría serla. Una solución a este tipo de problemas es recurrir a un método que se denomina encriptación. ¿Qué es encriptación?. Alterar el contenido de un archivo, por ejemplo, para hacerlo ininteligible a terceras partes no autorizadas mediante el uso de un código secreto. Por qué muchas personas no usan este método, no lo sé. Pero ahora por lo menos quienes nunca oyeron hablar de él ya lo saben. El contenido de un correo que ustedes están por enviar podría tener la siguiente frase:

"Quisiera que supieras que aquí estamos todos bien."

Este es el mismo correo pero encriptado:

--- COMIENZO DEL MENSAJE PGP ---

huafIOSDJ86NBjkhdJjkbns54ufhIUHDFuihws9-dhv653Gsoi8eHDIllhkdi

--- FIN DEL MENSAJE PGP ---

Ahora, ¿cuál correo cree usted que es más seguro?. ¿En cuál se animaría a mandar el código de acceso a su cuenta bancaria? ¿¿¿Cuál de los dos le gustaría ver a su esposo o esposa si le está enviando una carta a su amante???: (+ >)

Con programas que se encuentran disponibles, la encriptación y decriptación de correos y archivos se realiza en forma rápida y sin mayores problemas. La decisión de encriptación de los datos depende de qué tan importante sea la información ya que este proceso siempre usa algunos recursos de los sistemas y afecta el tiempo de respuesta.

CORTAFUEGOS PERSONAL

Ahora, vamos a darle una mirada a los Cortafuegos (firewalls). Su proveedor de Internet seguro tiene uno. Pero, ¿tiene USTED uno en SU máquina?, ¿lo tiene en SU red?

Si la cuenta no falla, hay más de 65 mil "PUERTOS" (PORTS), en efecto son puertos o puertas de entrada a su computadora. Por ejemplo, para mandar y recibir correos electrónicos, usted generalmente se conectará con otra computadora mediante los PORTS 25 y 110. Si se conecta a otra computadora para el intercambio de archivos utilizando un protocolo denominado FTP (File Transfer Protocol), usualmente utilizará el PORT 21. Los PORTS son puntos de acceso a su computadora usados por los programas y aplicaciones.

El mundo de las computadoras es como el mundo REAL. Cuanto más piensa en él, cuanto más se da cuenta que no es tan diferente, más se pone en posición de protegerse.

Si usted vive en un edificio de departamentos, incluso si su edificio tiene un guardia armado, ¿usted no cierra con llaves las puertas del departamento?. Claro. Por su puesto que lo hace. Pensando en todo esto, ¿por qué dejamos nuestras computadoras con las "puertas abiertas"?. Instale un cortafuegos personal. Su función es permitir el acceso a SU computadora a las personas y aplicaciones que USTED quiere que tengan acceso a SU información. Puede ser un programa o un equipo. Generalmente los equipos cortafuegos son utilizados por las grandes empresas mientras los programas son más de uso personal y para pequeñas y medianas empresas. Existen cortafuegos con muchas funciones que van desde controlar el tráfico hasta autenticar los usuarios para accesos a servicios específicos. Se usan comúnmente para proteger redes internas de accesos externos. También se pueden usar internamente dentro de una empresa para controlar acceso de red a departamentos específicos o recursos.

Ya hace varios años que este tipo de programas y equipos han estado funcionando, pero eran caros y complicados de usar. Hoy esto quedo en el pasado. Usted puede descargar fácilmente uno desde Internet y usarlo. Nosotros personalmente utilizamos el "Zone Alarm" y lo hemos estado utilizando desde hace algún tiempo. Ahora le toca a usted "bajarse" un cortafuegos, instalarlo y usarlo junto con sus correos encriptados.

PROTECCIÓN ANTIVIRUS

No hay NINGUNA razón para que alguien, o alguna computadora no cuenten con el servicio de un programa contra virus, instalado y actualizado regularmente.

Los antivirus son programas creados para contrarrestar la creciente oleada de programas dañinos conocidos como virus. Su nombre viene de correlacionar la forma en que estos se propagan. Son simples programas que al ser ejecutados pueden alterar la estructura del software del sistema o destruir programas o datos sin autorización y conocimiento del usuario. Una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema. De todas formas, dentro del término "virus informático" se suelen englobar varios tipos de programas, virus puro, caballos de Troya, bombas lógicas, gusanos, etc.

Un buen Antivirus constantemente está monitoreando tanto la memoria de su computadora como cualquier actividad que se esté realizando en su disco duro. Incluso pueden actualizarse automáticamente las veces que quiera y en el momento que usted le especifique. Si uno recibe generalmente una cantidad considerable de virus por semana. ¿Qué se podría pensar acerca de esto?. Yo diría que eso nos tendría que hacer ver que otras personas no están haciendo lo suficiente en lo que a protección antivirus se refiere. Pensemos que si todos hicieran algo esos mails con virus que nos envían a menudo, no podrían llegar a nosotros.

Tenga en mente que hay antivirus GRATUITOS disponibles en Internet.

Por último, la única forma de que los virus no sigan circulando por la red de redes es que comience cada uno de ustedes por usar un antivirus, por mantenerlo actualizado, los nuevos programas antivirus no requieren ningún tipo de intervención humana, configúrelo y olvídese.

CONCLUSIÓN

Quizás lo que hemos escrito anteriormente es solo una pequeña porción de todo lo que existe dentro del tema seguridad, y lo más probable es que sigamos tocando estos temas en próximas ediciones, pero es por lo menos la forma de comenzar, cada uno de nosotros deberíamos conocer por lo menos estos tres aspectos de la seguridad, la encriptación del correo, por ser la herramienta más utilizadas en la comunicación dentro de Internet, la utilización de cortafuegos para evitar accesos no deseados a nuestros recursos físicos y lógicos, y la protección antivirus, para prevenir de efectos no deseados principalmente en la información y programas que tenemos almacenados en nuestras computadoras.