SEGURIDAD BÁSICA EN INTERNET

Cortafuegos (Firewall)

Un cortafuegos (o firewall en inglés) es un elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

La instalación y uso de firewall tiene ventajas que repercuten en la seguridad general del sistema informático:

•Protege de intrusiones.- El acceso a ciertos segmentos de la red de una organización sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.

•Protección de información privada.- Permite definir distintos niveles de acceso a la información, de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.

•Optimización de acceso.- Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

Navegadores Web

Un navegador web (del inglés, web browser) es una aplicación software que permite al usuario recuperar y visualizar documentos de hipertexto, comúnmente descritos en HTML, desde servidores web de todo el mundo a través de Internet

Usar un navegador seguro y mantenerlo actualizado proporciona una base de seguridad mínima que facilita el trabajo a otros programas como antivirus o firewalls.

- Bloqueador de ventanas emergentes

Un Bloqueador de ventanas emergentes o Anti pop-up es un programa diseñada con el único fin de evitar, bloquear o no mostrar ventanas emergentes.

Correo Electrónico y Spam

El principal problema actual es el spam, que se refiere a la recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades, promoviendo Rolex, Viagra, pornografía y otros productos y servicios de la calidad sospechosa. Usualmente los mensajes indican como remitente del correo una dirección falsa. Por esta razón, es más difícil localizar a los verdaderos remitentes, y no sirve de nada contestar a los mensajes de Spam: las respuestas serán recibidas por usuarios que nada tienen que ver con ellos.

Además del spam, existen otros problemas que afectan a la seguridad y veracidad de este medio de comunicación:

- los virus informáticos, que se propagan mediante ficheros adjuntos infectando el ordenador de quien los abre
- el phishing, que son correos fraudulentos que intentan conseguir información bancaria
- los engaños (hoax), que difunden noticias falsas masivamente
- las cadenas de correo electrónico, que consisten en reenviar un mensaje a mucha gente; aunque parece inofensivo, la publicación de listas de direcciones de correo contribuye a la propagación a gran escala del spam y de mensajes con virus, phishing y hoax.

Servidores FTP

Un servidor FTP es un programa especial que se ejecuta en un equipo servidor normalmente conectado a Internet (aunque puede estar conectado a otros tipos de redes, LAN, MAN, etc.). Su función es permitir el intercambio de datos entre diferentes servidores/ordenadores.

El uso de servidores FTP sin seguridad no es recomendado, permite con mucha facilidad el acceso de intrusos desde el exterior (Internet) al interior de la red de la empresa con el consiguiente peligro que representa por fuga de datos sensibles o uso indebido de su sistema informático. El anterior mencionado SFTP añade un nivel extra de seguridad y encriptación que lo hacen más recomendable.