SEGURIDAD INFORMATICA PERSONAL I.

1.- Presentación / introducción

La siguiente explicación es una guía de referencia para usuarios de ordenadores personales, que tienen preocupación o interés en conseguir un mínimo grado de seguridad informática personal a la hora de poder contar con las nuevas tecnologías que nos rodean y que, cada día se hacen más imprescindibles para realizar cualquier tipo de actividad.

Esta charla no está dirigida específicamente a Administradores de redes corporativas o de telecomunicaciones, ni responsables de seguridad corporativa (aunque sí es aconsejable un pequeño repaso para éstos últimos).
Y no está dirigida a estas personas porque la charla tenga un bajo nivel técnico, sino porque las necesidades de unos y otros (administradores y usuarios comunes) son diferentes (y algunas veces contrapuestas).

Un administrador corporativo cubre sus necesidades de seguridad de manera muy diferente a como lo afronta un usuario, ya que tanto sus medios como sus conocimientos son los que le darán salida a sus posibles problemas de manera profesional.

Cuando un administrador se encuentra delante de un sistema, antes de llegar allí se ha formado y ha adquirido unos hábitos profesionales que le ayudarán a solventar sus necesidades.

Sin embargo, el usuario común, no acostumbra a dedicarse a la informática de manera profesional sino que su especialización será en cualquier otro campo, pero que lo desarrollará con las herramientas que la tecnología le ofrece.

Si el administrador de sistemas necesita colocar un cortafuegos (firewall), instala un ordenador y lo dedica exclusivamente a realizar esa labor, pudiendo acotar todos los posibles puntos débiles que no sean indispensables para el servicio que deberá de realizar esa máquina, que además funcionará con un Sistema Operativo (S.O.) con un grado de seguridad determinado.

Por contra el usuario normal, si quiere tener un cortafuegos deberá de instalarlo en su ordenador donde tiene instalado un antivirus, un navegador de internet, un cliente de correo electrónico, el FTP, el Netmeeting, el ICQ, etc...

Esta variedad de servicios corriendo en ese ordenador, cuyo funcionamiento el usuario desconoce, un sistema operativo que quizá no sea excesivamente seguro, y una política de seguridad mal establecida, hace que pueda ser vulnerable a diferentes tipos de *ataques*. Si es el portátil de una empresa, ese sólo ordenador puede estar comprometiendo seriamente la seguridad de toda corporación.

Bien, pero, ¿qué tiene mi ordenador para que lo quieran atacar y se aprovechen de sus vulnerabilidades?

1.- Seguridad personal básica informática (concepto)

El hecho de poseer o poder manejar un ordenador hace que, aunque sea mínimamente, dentro de él almacenemos datos.

Por muy insignificantes que a veces nos parezcan, estos datos hablan de nosotr@s o bien de otras personas.

En España existe una normativa, Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD), que penalizaría nuestra actuación en caso de que nos sustrajeran información sobre otras personas.

La seguridad personal sería el método por el que nos protegeríamos de miradas indiscretas, o accesos no permitidos a nuestro ordenador o a los datos que en ellos almacenamos.

Lo que a nosotr@s puede no parecernos importante, a otr@s sí puede parecérselo.

Si queremos *conscientemente* estar segur@s de tener nuestra información a salvo, deberemos ser conscientes de lo que hacemos con ella, de dónde la dejamos, cómo la guardamos y a quién y de qué manera se la ofrecemos.

Hay empresas que están llegando a pagar 500.000 Pts. por cada perfil de usuario de Internet de un determinado tipo que le suministren.

Estos días asistimos atónitos, viendo como empresas.com están vendiendo sus bases de datos de carácter personal al mejor postor.

Otras veces podemos estar interesados en mantener un cierto anonimato en determinadas acciones que podría quebrantarse por un fallo en la seguridad.

2.- Seguridad física.

El ordenador más seguro es aquel que se encuentra encerrado en una habitación infranqueable y está desconectado.

Si realmente se quiere hacer daño a los datos, lo más rápido y eficiente es sustraer los discos duros y cualquier tipo de material de soporte e inutilizarlos concienzudamente.

La seguridad física del ordenador está en el hecho de hacer inaccesible físicamente (no sólo que no se pueda utilizar) el ordenador a un posible intruso, evitando que pueda sustraerlo, estropearlo, o llegar a percibir cualquier tipo de información proveniente tanto del aparato como del usuario a la hora de relacionarse con él.

El mejor sistema de seguridad física es el que obtengamos despues de un minucioso estudio de la situación.

Se puede extraer información de lo que realiza un ordenador desde distancias que realmente no sospechamos, una pantalla es legible para según qué cosas desde unos 3 metros de distancia (más si hay gráficos x Ej.).

Las señales electromagnéticas que emite el ordenador o la pantalla también pueden captarse. Este método de *espionaje* recibe el nombre de **_Técnica tempest_**??.

Puedo hacer grandes inversiones en construir una sala muy espaciosa y en el centro colocar el ordenador (cuanto más alejado de paredes y ventanas más difícil será colocar un *chivato*), la sala la blindo con paredes de 2 mts de grueso de acero y la forro con una malla para construirle una jaula faraday (para evitar la propagación de ondas electromagnéticas). Si establezco una comunicación vía voz o datos por teléfono y me pinchan la línea en el exterior, en ese momento la seguridad interna queda quebrada por la externa.

Otro ejemplo habitual en los últimos días es la pérdida de ordenadores en aeropuertos, taxis, el tren. Un dato curioso es que, según las noticias de los medios, parece ser que los más propensos a perder este tipo de artilugios son precisamente profesionales de la seguridad (agentes del MI5, CIA, FBI, etc...).

Como se ve hay diferentes maneras de ser vulnerables a la perdida de nuestra información.

Hay una solución que, a pesar de no ser la única que deberemos de utilizar, sí ha de ser la que tengamos más en cuenta, y es la ***copia de seguridad*** o también llamada Backup. De manera abreviada diríamos que un backup es una copia de todos nuestros datos pasandolos a algún tipo de soporte de almacenamiento (disquete de 1 a 200 MB, CD-ROM, cinta, servidor de backup, etc).

Un Backup exige niveles de seguridad física parecidos a los de nuestro ordenador.

ORDENADOR PERSONAL, PC

(LOCAL)

1.- Seguridad hardware (BIOS y otros).

Es la que utiliza maquinaria física para funcionar.
La seguridad con hardware puede llevarse a extremos muy sofisticados, como podrían ser controles biológicos (huellas, ojos, manos, voz), para poder controlar los accesos al ordenador.

Normalmente tienen un sobrecoste sobre el ordenador por lo que se tiende a no utilizar este posible método (salvo cuando la relación *precio/importancia de la información* es favorable).

Aparte de estos métodos, a la hora de interceptar el acceso a nuestro PC o portátil podemos contar con los que nos vienen de fábrica y no deberemos de pagar por ellos.

Password de BIOS
Se accede a través del menú de setup de la BIOS cuando el ordenador empieza a arrancar pero todavía no ha empezado a cargar el S.O. (en la pantalla normalmente nos sale un aviso: **Press Delete Key to enter Setup**
Nos permite poner passwords para usuario y para administrador, para entrar al sistema o para acceder al setup de BIOS.

Si elijo la de sistema, el sistema operativo no empezará a arrancar hasta que introduzca la palabra correcta:

Algunas de sus vulnerabilidades son:

- Si se dispone de tiempo suficiente y cierta intimidad, acceder a la tarjeta donde se encuentre la BIOS y resetearla (se perderá la configuración BIOS y por tanto el password).

- Utilizando alguna de las claves maestras de las BIOS más utilizadas.

- Atacando la BIOS desde un disquete o programa.

- Probando posibles passwords, ya que no tiene límite de errores.

Bootdisk desde C:

Podemos configurar la BIOS para que el arranque del sistema se inicialice desde la unidad que queramos: disquete, disco duro, CD-ROM, o cualquier otro dispositivo que sea compatible con nuestra BIOS.
Si anulamos el arranque desde disquete, nos aseguramos que no podrán arrancar con un disquete de sistema y saltarse posibles barreras que tengamos instaladas.

También nos evitará problemas con virus en sectores de arranque de disquetes.

2.- Seguridad del Sistema Operativo.

El sistema operativo es el programa que hace que nuestro ordenador funcione. Existen diferentes sistemas operativos algunos de ellos libres, unos más seguros que otros, aunque todos son vulnerables (unos más que otros por supuesto) y en ello no interviene su precio.

El sistema operativo para referirnos en los ejemplos será mayoritariamente Windows 9x pues es el sistema más establecido tanto en usuarios domésticos como en empresas (aunque es un sistema operativo para el hogar).

La seguridad de un sistema operativo empieza básicamente en su sistema de ficheros, en cómo almacena estos ficheros.

Los sistemas operativos que se consideran medianamente seguros son aquellos que permiten establecer políticas de acceso a los datos y a los recursos, y sus ficheros pueden tener propietario, eligiendo éste el uso que harán los demás usuarios.

Tabla 1- Sistemas operativos

NO SEGUROS	SEGUROS
MS-DOS	UNIX
MAC-OS	NOVELL
WIN-3.X	BSD
WIN95 – 98 - ME	WIN NT
	WIN 2000
	LINUX (libre)

3.- Contraseñas.

Gran parte de la seguridad en muchos sistemas informáticos y electrónicos depende de la contraseña. (ordenadores, móvil, tarjeta bancaria, ...)

Una contraseña es más segura cuanto más tiempo se tarda en romper.
Cuanto más complicada es una contraseña, más tarda en romperse.
Todas las contraseñas se pueden romper, sólo es cuestión de tiempo y medios.

Contraseña pobre:
Uno de los errores más comunes a la hora de crear una contraseña es la de "hacerla facilita que tengo mala memória"

- 26 posibilidades en letras mayúsculas.
- 26 posibilidades en letras minúsculas.
- 10 posibilidades en números.

(contraseña: 7491) 10 x 10 x 10 x 10 = 10.000 posibilidades
(contraseña: mama) 26 x 26 x 26 x 26 = 456.976 posibilidades

10.000 posibilidades suena a mucho, pero si tengo el tiempo suficiente puedo ir probando una a una cada una de sus posibilidades.

Una contraseña un poco más útil:
Una contraseña medianamente segura, constará de no menos de 8 caracteres, entre los que se intercalarán mayúsculas, minúsculas, números y signos o espacios, vendría a ser:

- 26 posibilidades en letras mayúsculas.
- 26 posibilidades en letras minúsculas.
- 10 posibilidades en números.
- de 15 a 36 posibilidades en símbolos (depende de la aplicación) &¡'º<_-)(

26 + 26 + 10 + 15 (x ej.) nos da un alfabeto de 77 caracteres.

Con una contraseña de 8 caracteres tenemos 77^{8} posibles contraseñas o lo que es lo mismo 1,235736291548e+15 (más de un trillón de posibilidades).

Los microprocesadores actuales realizan millones de procesos por segundo, romper contraseñas es una cuestión de tiempo y paciencia.

Muchos de los ataques que se producen a los servidores de Internet y de redes son para conseguir la lista de contraseñas que acostumbran a guardar los S.O. para reconocer a sus usuarios. Poder actuar en el sistema como un usuario normal y sobre todo como el administrador es su objetivo prioritario

Una vez que se tiene una lista con contraseñas se la somete a un ataque de comparación con contraseñas, que tu le suministras; éste ataque suele realizarse de 3 maneras básicamente:

- Ataque de diccionario (comparar una lista de palabras)
- Ataque de fuerza bruta (comparar una a una cada una de las diferentes posibilidades)
- Ataque mixto (empiezas con el diccionario y acabas con la fuerza bruta)

La mayoría de los sistemas operativos tienen soporte para contraseñas de 14 caracteres, que si hacemos un pequeño cálculo nos ofrecen: 77^{14} que es igual a 2,575550990467e+26 posibilidades (más de 2.500 cuatrillones)

Para romper la contraseña con un PC familiar es necesario dejarlo funcionar durante bastantes días.

Una de las bases de la seguridad es tener en cuenta la inversión y esfuerzo que se ha de realizar para superarla, en tiempo y medios, y las consecuencias que se derivan de ello.

No me sirve de nada coger el fichero de contraseñas de un sistema, si ellos tardarán 3 días en darse cuenta de la intrusión y yo 1 semana en romperlo una contraseña; mientras no he trabajado ni ¼ parte en el fichero, el administrador del sistema habrá cambiado las contraseñas por otras nuevas.

Y volveré a estar como antes, sólo que el administrador ya sabrá por dónde entré y ...

4.- Paquetes básicos.

Entre los paquetes básicos con los que podemos contar en un ordenador personal con tal de disfrutar de un mínimo de seguridad podríamos destacar:

- Contraseña del sistema.
- Administrador de Usuarios y perfiles.
- Poledit
- Contraseñas de programas comunes.

CONTRASEÑA DE WINDOWS:

Windows 9x nos permite controlar el acceso al sistema mediante contraseñas de usuario. Esta contraseña puede constar desde 0 a 14 caracteres a elegir entre letras, números y algunos signos.

En su ***configuración inicial***, tiene dos grandes inconvenientes:

A.- La contraseña presenta las opciones de aceptar, cancelar. Si se elige la opción cancelar, nos permite entrar sin ningún tipo de restricción al sistema (esto no ocurre en sistemas como NT, UNIXES, y otros)

B.- Antes de llegar aquí, interrumpiendo el arranque normal del sistema, podremos acceder al ordenador en modo MS-DOS en consola de comandos. Con un poco de conocimiento de MS-DOS se puede acceder a todo el disco duro.

Administrador de usuarios y perfiles

El administrador de usuarios nos permite crear vistas y lugar de almacenamiento de datos personalizados, dónde guardar los documentos, el escritorio, salva pantallas, etc.; para cada uno de los usuarios que creemos.

Permite también la creación de algunas políticas de seguridad restringiendo el acceso a algunos elementos del sistema. Su seguridad depende, además de la configuración del perfil, en la seguridad de la contraseña de Windows antes mencionada.

En los sistemas seguros como NT, UNIXES y otros, es difícil saltar este tipo de restricciones, sólo el administrador es el autorizado para realizar cambios de privilegios en el sistema, (de ahí ese afán por los listados de passwords)

Poledit

Poledit es una herramienta administrativa que nos facilita Microsoft para establecer políticas de sistema sobre los usuarios y sus perfiles. Acostumbra a venir en el CD de instalación del sistema operativo Windows 9x. Cuando lo hemos instalado en \Menú Inicio\Programas\Accesorios\Herramientas del sistema nos aparecerá un nuevo programa llamado **Editor de planes de sistema**

Acostumbran a utilizarlo los administradores de sistemas informáticos, su función es la de poder manipular el registro de Windows, de una manera más visual y entendible.

Con Poledit se puede llegar a marcar políticas de seguridad muy férreas para un usuario determinado. Se puede llegar a hacer útil la contraseña de Windows. Y cuando se utiliza en red con un servidor de autentificación y perfiles asegura estándares de configuración.

Sus debilidades siguen siendo el paso previo por MS-DOS, el conseguir los ficheros de contraseñas de los usuarios y la posible variación del registro de windows (uno de los puntos más vulnerables) y que se encuentra desperdigado por el sistema en varios ficheros.
Una vez conseguido el fichero de contraseñas, el enfrentarlo a un ataque con cualquiera de los numerosos programas que existen, es como hemos explicado anteriormente, una cuestión de tiempo.

Programas comunes

Dentro de los paquetes informáticos comunes nos encontramos con las herramientas más utilizadas, entre estos destaca el Office. Paquetes de programas como Word-Perfect, Star Office y otros también ofrecen las mismas funcionalidades.

Muchas personas utilizan este paquete de programas con un rendimiento muy bajo sobre las posibilidades que ofrece, y una parte poco utilizada es por supuesto la de la seguridad.

Los programas Word, Excel y Access nos ofrecen la posibilidad de introducir una contraseña para evitar el acceso al documento. Para leerlo o para modificarlo. En Excel incluso puede llegar a asegurarse una celda determinada de una pagina de un libro.

El problema que presentan es el sistema de encriptación de la contraseña, que al ser propietario, no se permite mejorarlo libremente, lo que hace que con el tiempo vayan apareciendo programas para *adivinar* las contraseñas de estos documentos.

5.- Encriptación y métodos de camuflaje.

Encriptar (hacer críptica) o cifrar una información consiste en poder variar los elementos del mensaje de manera que este quede ininteligible para un ser humano normal y además, el método, nos permita restaurar la información original cuando queramos, y sólo para quien queramos.

Cuando pensamos en el peligro de que alguien pueda acceder a la información que guardamos en nuestro ordenador, o que nos intercepten los correos electrónicos (como veremos más adelante) la encriptación (o cifrado) es uno de los mejores métodos para evitarlo.

Puede llegar a ser tan buen método para salvaguardar la información que en muchos países su uso es ilegal, y en otros está restringido en algunos aspectos (el Reino Unido obliga a sus ciudadanos que tengan programas de encriptación a entregarles una copia de sus claves privadas so pena de ir a prisión). Muchos países lo consideran un arma de guerra y hasta hace muy poco EEUU salvaguardaba al mundo de estas armas prohibiendo la exportación de programas con un nivel de encriptación mayor de 48 bits (la longitud de la clave), cuando ellos podían usar claves de mayor rango.

En el momento de escribir estas notas, la Unión Europea está a punto de adoptar un plan de inspección de sus sistemas de seguridad, pues temen que cuando le pidieron lo mismo al FBI de EEUU, éstos pudieran haber instalado algún dispositivo que vulnerara la seguridad de los sistemas de seguridad de la UE.

Incluso acaba de salir una recomendación de la UE sobre el uso de la encriptación de la información

Existen diversos programas y maneras de cifrar nuestra información. En líneas generales la mayoría de ellos lo que hace es que a través de un algoritmo se crea una clave de un tamaño determinado (cuanto más larga, más compleja será la posibilidad de romper la clave) que servirá para sustituir las unidades de información del mensaje por otras generadas gracias a la clave. Y para descifrarlo pues hace el proceso al revés (siempre que se sepa la clave).

De todos estos programas, el más famoso y utilizado es el PGP (Pretty Good Privacy **Privacidad Bastante Buena**). Phill Zimmerman (su inventor inicial) tuvo que soportar una investigación a fondo de su persona por el Gobierno Federal de los EEUU. Gran parte de la popularización de estos programas se la debemos a los defensores de las libertades, personajes no gubernamentales, que llevan batallando contra el gran hermano desde hace bastante tiempo. También existen otros programas de software libre como GNU-pgp (PGP sólo es gratis si no lo utilizas para ningún uso comercial).

El funcionamiento de PGP es muy sencillo una vez lo tienes instalado. Aunque el programa funciona en inglés, no es difícil hacerse con alguna guía en castellano que nos pueda guiar paso a paso (kriptopolis tiene una).

Una vez instalado el programa nos pedirá que creemos nuestra llave, y podremos elegir crearla con diferentes algoritmos y longitudes. Como que el programa da mucha importancia al password que le pongamos a la clave, tiene un indicador, que nos señala el grado de seguridad del password que estamos escogiendo para realizar la clave. Una vez concluido, dispondremos de 2 llaves, una pública, que será la que enseñaremos al mundo y que todos podrán tener si quieren, ellos la utilizarán para enviarnos los mensajes cifrados a nosotros. La otra llave es la privada, y es la que utilizaremos para descifrar los mensajes que alguien nos haya cifrado usando nuestra llave pública.

La verdad es que en esto de la encriptación, lo más difícil es entenderla, porque usarla se ha convertido en una función muy fácil. PGP utiliza unos plugins que se instalan en los clientes de correo más utilizados, y con sólo darle a un botón, nos cifra el mensaje que estemos escribiendo, sólo debemos decirle al programa qué llave pública usaremos (de quién) para que sólo esa persona que dispone de la pareja privada de esa llave pueda leerlo.

También puede firmar los mensajes, es decir, el mensaje es visible para todo el mundo que acceda a él, pero al comprobar la firma nos avisaría si alguien lo ha manipulado antes de poder leerlo.

También se puede encriptar cualquier fichero con tan solo pinchar sobre él con el botón derecho del ratón y elegir esa opción.

Todas estas funcionalidades están haciendo, sin embargo, que últimamente se le hayan descubierto agujeros importantes de seguridad a estos programas, que los han hecho vulnerables, los algoritmos con los que se crean siguen siendo imposibles de romper en la practica, pero los programas que los implementan son los que abren la vulnerabilidad del método empleado.

Otro método para poder hacer correr nuestra información es la técnica que utiliza la **esteganografía**. Consiste en mezclar los bits de la información que nos interesa con los bits de un fichero convencional, los más utilizados son ficheros de sonido y de imagen. Una vez acabado el proceso, el fichero de imagen sonará igual, al menos para la percepción normal del oído humano. Si el fichero es de imagen pues tampoco se notará ningún cambio a simple vista.

Esto es así, porque el proceso recoge la información original y después de encriptarla la va colocando en bites poco significativos de la información del fichero destino, una ligera variación en bites poco significativos en un fichero de audio o de imagen, produce cambios que normalmente no estamos en disposición de notar, y más si no podemos contrastarlo con un original.

SEGURIDAD INFORMATICA PERSONAL II.

(INTERNET / INTRANET)

En la anterior explicación se consideraba la posible vulnerabilidad ante los peligros locales que pueden afectar a nuestro ordenador y a nuestra información.

En la que sigue intentaremos hacer un pequeño recorrido y de manera general sobre los puntos a tener en cuenta cuando nuestro ordenador empieza a contactar con otros a través de redes.

Cuando estamos conectados en red, en el trabajo por ejemplo, acostumbramos a utilizar recursos unos de otros, impresoras, archivos, servicios como correo, web, o bases de datos. Para ello los ordenadores se intercambian información a través de un cable (hoy día empiezan a extenderse las redes wireless [sin cables, por ondas, que las hacen más vulnerables]) y nuestra información corre por un camino hasta que llega a su destino, y para ello deben de darse ordenes entre los ordenadores para dar permiso o no a según que tareas necesarias para la labor.

Esto que hace que nuestro trabajo sea más productivo y agradable, también hace que nuestro proceso sea más vulnerable, pues la información que corre a través de un cable se puede recoger (sniffing) y analizar, y con la información recogida incluso utilizarla para conseguir más información (contraseñas, métodos, etc).

Una carpeta puesta a compartir alegremente en una red puede hacer que un intruso pueda ver todo lo que tengamos en el ordenador, e incluso llegar a instalarnos alguna herramienta (troyanos, keylogers, capturadores de sesión, ...) para facilitarle más su intrusión.

Los ordenadores se comunican por la red a través de protocolos y producen unos servicios determinados según los preparemos para ello o no. Por ejemplo, si quiero consultar mi correo electrónico de la empresa (que tiene una Intranet), abro mi cliente de correo y le digo que vaya a buscar mi correo nuevo, el cliente de correo a través de su programación empieza a generar una petición y la envía a través de un puerto de mi pc al puerto 110 del ordenador que en la empresa se dedica a dar el correo. El hecho de que vaya directamente al puerto 110, es porque es un estándar establecido, que viene a decir que quien da el servicio de entrega de correo (POP3) lo hará a través del puerto 110, por lo que ese puerto siempre estará activo y a la espera de recibir conexiones.

El hecho que un servicio corra en un puerto determinado hace que cualquier ordenador pueda conectarse a ese puerto e intentar comunicar con él, pudiendo incluso quebrantar su funcionamiento debido a fallos en la programación de ese servicio, lo que vienen a llamarse los bugs o vulnerabilidades, e incluso llegar a poder penetrar en el sistema y gobernar el ordenador.

Cuando estamos en una red con un puerto a la escucha, un recurso a compartir, o con software con fallos conocidos, somos propensos a que entren en nuestro sistema.

Algunas herramientas que un intruso podría instalar en nuestra máquina, además de virus podrán ser:

Un troyano, que es un programa que abre servicios en un ordenador para poder ser utilizado en la distancia, por control remoto. Al igual que un servidor web recibe ordenes de ofrecer páginas http, un troyano ofrece todo aquello para lo que se programó, y actuará en el ordenador cliente como si quien le diera las ordenes estuviera sentado al teclado. Un troyanos famoso es el netbus , que dejaba anodada a la pobre víctima cuando esta veía que su CD-ROM se abría, aparecían mensajes en la pantalla, se abrían carpetas, se apagaba el ordenador, etc.

Un keyloger es un programa que monitoriza todas las ordenes que se le dan al teclado (contraseñas por ejemplo) y lo va guardando todo en un fichero, luego solo debe de abrirse en un procesador de texto y sabremos todo lo que se ha tecleado en el ordenador.

Un capturador de sesiones es un programa que va tomando instantáneas de la pantalla y también puede que las pulsaciones del teclado y las almacena para después poder consultar qué programas se han abierto, qué se ha hecho con ellos y qué se ha tecleado.

Los antivirus más utilizados acostumbran a detectar también troyanos y keylogers (no todos). Una buena manera de evitar estos sobresaltos, es tener instalado un cortafuegos (firewall), que estaría controlando en todo momento qué es lo qué quiere salir y qué es lo que quiere entrar de nuestro ordenador, pudiéndose configurar a nuestras necesidades.

1.- Navegar en la WWW (cookies, scripts, cgis,...).

Navegar por la World Wide Web (www) es un servicio que prestan algunos ordenadores que están conectados a Internet y son esas páginas llenas de colores, dibujos, sonidos, etc.

Es uno de los recursos más novedosos, ya que aunque Internet empezó a gestarse en los años 60's, el browsear (de browser) data 1992, y aun siendo el más nuevo, es el servicio más utilizado por la gran avalancha de usuarios de internet de los últimos tiempos. Se basa en el protocolo de hipertexto (http Hypertext protocol), es aquel servicio que hacemos correr cuando abrimos el Internet Explorer, el Netscape Navigator, el Opera, etc., y nos vamos a http://www.mi-pagina.com.

Su funcionalidad deja bastante que desear para los usuarios domésticos que hacen uso de líneas telefónicas normales, y estos documentos al estar cargados de gráficos, sonidos y animaciones, hace que lo que es fundamental en Internet (la información), cada día más vaya brillando por su ausencia, pasando a ocupar su lugar temas de comercio y entretenimiento, sobre todo enfocado a las masas (como la televisión).

Pero esta utilidad tan atractiva y novedosa no deja de tener su problemática como casi todo en el mundo de la informática.

Los peligros a los que estamos expuestos a la hora de utilizar un navegador (sobre todo los más conocidos) son:

1.- Comunicación en texto plano, quien intercepte la comunicación podrá leerla sin ningún problema, lo que se agrava a la hora de rellenar formularios o enviar información confidencial a alguna página. Esto acostumbra a evitarse en cierto grado cuando se usa protocolo de encriptación y lo reconoceremos porque si no lo hemos deshabilitado, a la hora en que la página empieza a cargarse veremos una ventana que nos informará de ello (va a entrar usted en un lugar seguro...), o bien aparecerá un candado cerrado en la barra inferior del navegador.

2.- Ofrecimiento gratuito de nuestros datos al administrador del web que visitemos. Esto se produce por vulnerabilidades en la programación de los navegadores, que posibilita, o posibilitaba, el saber la identidad electrónica del visitante con tan solo pasar el ratón sobre un link o pulsando un botón. O incluso preparando un pequeño escript (programa) que le ofrezca dicha información, pudiendo llegar a ver todo nuestro disco duro. Hay que saber que el explorador acostumbra a funcionar en nuestro sistema con privilegios de alto nivel, haciéndolo incluso en sistemas de alta seguridad como windows nt o 2000.

3.- Ataques premeditados con ficheros maliciosos. Se producen cuando accionamos algún link en una página que enlaza con un fichero ejecutable como virus, troyanos, etc. Un ejemplo podría ser que accionemos un link que apunta a un documento de Word infectado con un virus de macro. Al accionar sobre el link, y al tratarse de un fichero **amigo** de Microsoft, éste en vez de bajarse a nuestro disco, automáticamente abre el Word, se ejecuta y ya estamos infectados.

4.- DOS a nuestro pc (Denial Of Service, denegación de servicio). Se puede realizar a través de otros servicios también. Es lo que acostumbra a decirse que el ordenador **se ha quedado colgao**. Es mantener a nuestro ordenador trabajando al 100% de uso de procesador para intentar dar una respuesta al ordenador atacante, sin tener tiempo de procesador para ninguna tarea más. El sistema se cuelga.

5.- Scripts maliciosos que son aquellos ficheros que aunque no son programas, son rutinas ejecutables con un motor de ese lenguaje que tengamos en nuestro odenador. Visual Basic es un lenguaje de programación que utiliza scripts, y windows es la plataforma ideal para hacer correr el Visual Basic. También hay scripts para casi cualquier programa: Photoshop, Corel Draw, Office y sus macros, etc.

JAVA es un lenguaje de programación inventado por Sun. Hay sistemas operativos, electrodomésticos y otros que funcionan con java. Su característica en nuestro caso consiste en que aumenta el nivel de interactividad en las páginas web. Cuando ejecutas un link, un botón o menú desplegable en una página web (cada día hay más páginas que los usan), el servidor de esa página nos introduce un fichero en el ordenador con unas sentencias en lenguaje java, nuestro ordenador lo entiende y lanza nuestro motor de lenguaje java que viene con nuestro sistema y ejecuta el programa. Imaginemos lo que puede llegar a a hacer un webmaster malintencionado ya que cuando se ejecuta no sabemos qué es lo que ejecuta.

ACTIVEX son, como el caso de java, pogramas que te instalan los servidores en tu ordenador y se ejecutan. Las actualizaciones en linea que se realizan en el sitio de Microsoft (Windows Update) se hacen con controles activex. Su peligro es mayor que java, pues tiene permisos de muy alto nivel en el sistema llegando a trabajar en ring 0; Sun en este caso fue un poco más precavida que Microsoft. Normalmente vienen con un certificado para saber quien lo fabrico. Hace un par de meses a Micrososft le robaron diversos certificados.

Las **Cookies** son pequeños ficheros que nos instalan en nuestro pc los servidores, y sirven para guardar información de lo que hacemos en un sitio. Qué páginas elegimos, resoluciones, etc. Teóricamente solo debe de guardar eso, y teóricamente sólo sirve para ese sitio, pero es común hoy día, que una cookie puesta por un servidor la pueda leer otro, lo que nos produce una falta de privacidad personal, nadie tiene por qué saber a qué sitios voy y qué visito en ellos.

Funcionalidades parecidas pueden llegar a alcanzarse con las presentaciones flash, las transmisiones para windows media player, y otros muchos más.

Tanto Netscape como Iexplorer nos permiten habilitar y deshabilitar cookies, controles activex, java, scripts, ejecución de comandos, etc.. Sin embargo ello puede hacer que algunas páginas web no se vean como debieran e incluso que se nos deniegue el acceso a alguna de ellas.

A pesar de la constante actualización de las versiones de los navegadores, se ha de tener en cuenta que a los pocos días (o antes) de sacar una nueva versión, ya se descubren nuevos agujeros de seguridad en ellos.
Hay quien se pregunta si todos esos agujeros (que a veces se niegan en reparar) no los dejarán a propósito.

Los navegadores acostumbran a tener alguna opción de actualización, (en IE Herramientas/windows update) que nos llevará a una página oficial del navegador, en donde nos testearán y nos aconsejarán sobre las últimas actualizaciones para hacer más ¿seguro? el navegador.

2.- Correo electrónico

Quizá el mejor sistema de comunicación en la distancia. Escribimos un mensaje y a los 10 segundos el destinatario ya puede leerlo.

Sin embargo es una de las puertas de entrada a nuestra intimidad más utilizada en la era Internet.

Spam (correo no deseado), virus, troyanos, e incluso “amenazas anónimas” son cosas con las que diariamente nos podemos encontrar a la hora de abrir nuestro correo.

El hecho de tener configurado un cliente de correo hace que esta dirección la vayan recaptando a través de tu ordenador, visitando páginas web, rellenando formularios, enviando mensajes a grupos o listas de correo, etc.

Una vez nuestra dirección entra en el juego de la venta de datos, cualquiera puede comprarlos y hacer con ellos lo que quiera, desde asetearnos a correos no deseados a cruzarlos con otros bancos de datos, ampliando su conocimiento sobre nosotros.

Cuando se recibe correo no deseado y en el se da alguna dirección para desuscribirse, no es aconsejable hacerlo, pues muchas veces solo sirve para asegurarle al spamer que nuestra dirección sí existe y está activa, y así nuestra dirección adquiere todavía más valor para el spamer.

Otro de los peligros del correo es la llegada de los virus, que acostumbran a llegar en ficheros adjuntos y con nombres sugestivos o amigables (ingeniería social). Muchas veces ocurre que además nos lo envía alguien a quien conocemos, por lo que la confianza aumenta (más ingeniería social). O resulta ser una actualización o parche para un programa. Cuando lo accionamos, al ser un ejecutable, lanza sus rutinas e infecta nuestro sistema, realizando las acciones para las que fue programado.

Las acciones pueden variar, desde ejecutar una simple molestia de vez en cuando (un mensaje en la pantalla, iconos que se mueven, etc...) a hacer desaparecer completamente nuestra información e inutilizar el ordenador e incluso otros periféricos.

Esos ficheros acostumbran a ser ejecutables o scripts maliciosos, sus extensiones normalmente son: *.exe, *.com, *.bat, *.pif, *.vbs, *.vbe, y otras muchas más.

Debido a la interacción con la que cuentan los modernos y completos clientes de correo actuales, hace que cada día éstos sean más vulnerables, ya que heredan gran parte de las vulnerabilidades de otros servicios del sistema, como por ejemplo, Outlook Express, que puede ejecutar scripts en un correo con tan solo intentar leer el mensaje, vulnerabilidad que hereda del Internet Explorer.

3.- Virus y antivirus.

Los virus son programas y por lo tanto, no actúan hasta que son ejecutados. Acostumbran a venir en algún mensaje de correo aunque también venían en disquetes y CD's. Acostumbraban a ser ficheros ejecutables con extensiones *.exe, *.com, *.bat.

Con la interoperabilidad y interactividad de los nuevos sistemas operativos, los virus, como sus semejantes biológicos, se han perfeccionado, y se han adaptado a las nuevas circunstancias, aumentando los diferentes tipos y métodos de infección. Scripts de visual Basic, de java..., nos llegan en teóricos ficheros de juegos, salva pantallas, fotografías...

Y las últimas novedades son virus que se ejecutan con tan solo abrir el programa de correo que al querer visualizar un mensaje ejecuta un script que nos conecta con una web desde donde se actualiza o carga y se ejecuta, reenviándose a toda nuestra libreta de direcciones de correo (reproducción), al tiempo busca en nuestro disco información como claves de acceso a Internet, a bancos, cuentas corrientes, o lugares privados de la red, enviando toda esta información a algún lugar de Internet, pudiendo, una vez acabado su trabajo borrar nuestro sistema.

El daño que pueden realizar varía desde aquellos que solo son una broma o una pesadez molesta, hasta aquellos que borran todos nuestros datos y pueden inutilizar nuestro ordenador.

Últimamente va aumentando los tipos de virus que cuando infectan a un ordenador, una de las primeras acciones que realizan es la de buscar información privilegiada como nombres de usuarios y claves de cuentas de acceso en web bancarias, de inversiones, etc. Con el peligro que ello conlleva sobre nuestra intimidad.

4.- Troyanos y servidores. Espyware

Los troyanos, aunque se les puede incluir en la categoría de los virus, pues algunos pueden efectuar destrozos en nuestro sistema, tienen como objetivo principal el abrir tu ordenador a algún intruso.

Acostumbran a ser ficheros, que recibimos bien por correo o que nos bajamos de alguna web creyendo que es un programa (y puede llegar a serlo incluso).
Cuando ejecutamos el troyano, lo que normalmente acostumbran a hacer, es instalarse de manera definitiva en el sistema y reenviarse a toda la libreta de direcciones (reproducción), y avisa a alguien que está activo, enviando un mensaje de correo, o conectándose a través del IRC entre otras posibles.

Su misión es abrir un puerto en nuestro ordenador a través del cual ofrecerá un servicio bien de servidor o ftp o bien de control remoto, estando nuestro pc en manos del intruso.

El spyware además de funcionar en páginas web, también podemos introducirlos en nuestro ordenador a través de programas del todo inofensivos. Muchos programas que son gratuitos en la red, pueden ser gratuitos porque aunque no cobren dinero por el programa, si cobran por la información que ese programa, y sin que nosotr@s nos demos cuenta, va enviando a ciertas empresas cuya función es recolectarlos, crear los perfiles determinados y luego venderlos a otras empresas para otros fines.

5.- Internet Relay Chat (IRC).

Internet Relay Chat (IRC) es un servicio más que nos prestan los ordenadores gracias a Internet. En un principio consistía en poder comunicarse entre sí personas que conectaban con un servidor IRC y elegían una temática (un canal), allí podían expresar en línea sus ideas, apareciendo lo que escribían en una especie de pizarra. Hoy día, además es posible chatear en privado, intercambiar ficheros (hacer de servidor), oír música en el canal, etc.

Todo esto hace que se abran servicios en nuestro ordenador, que a veces no sabemos controlar, pero que otros si pueden o bien se aprovechan de ellos.

En el IRC además de charlar, es muy normal jugar a ***sacarse del canal*** un@s a otr@s, para ello existen comandos, que algunos programas incorporan o se pueden instalar con un script para el programa.

Los clientes de irc pueden recibir ficheros automáticamente si no están bien configurados. O actuar de servidor sin nosotros darnos cuenta. Lo que nos hace un buen juguete en manos cualquier desaprensivo sino vamos con cuidado.

6.- Firewalls.

Para poder intercambiar información a través de algún tipo de red sea esta corporativa, casera o internet (entre otras), es necesario que los ordenadores se comuniquen entre ellos.

Lo que hace un firewall es controlar todo aquello que entra o sale de nuestro ordenador.

Este control lo puede hacer a nivel de programas, dejando a unas aplicaciones sí y a otras no el poder intercambiar información.

También se puede filtrar por puertos de comunicaciones (si tengo un servidor que sólo va a comunicarse a través del puerto 80 (http x ej.), puedo deshabilitar todos los demás y así asegurarme que la comunicación sólo se establecerá por ese puerto.

También puedo establecer que a mi ordenador se conecten sólo desde una dirección IP en concreto o nombre de máquina y ninguna otra más, evitando las conexiones desde cualquier otra dirección o nombre de máquina.

También puede filtrarse por tipo de información que vaya encapsulada en los paquetes que se transmitan los ordenadores, etc.

Los firewalls pueden ser de diferentes tipos, de HIERRO, que son máquinas dedicadas a esa función exclusivamente y que cuentan en su interior con un programa al efecto. Y también pueden ser simplemente software, corriendo en un ordenador y que realizará las funciones de filtrado.

7.- Anonimizadores.

Como que cuando navegamos por la red hay la posibilidad que los sitios que visitamos vayan recolectando información sobre nosotros, nuestras direcciones de conexión (con quien me conecto INICIA, TERRA, etc), nuestro correo electrónico, nuestro país, nuestro idioma, nuestra edad, y un sin fin de riesgos con los últimos programas spyware en web, se crearon servicios en Internet que de alguna manera nos hace anónimos en la red (no invisibles).

La función consiste en que cuando quiero ver una página web de lo que sea, en vez de ir directamente a esa página web, paso por un servidor de anonimicidad, y desde allí visito la página que realmente me interesa.

Cuando llegue a la web que quiero, ésta recibirá los datos de ip, correo, etc., de la web de anonimicidad y no la mía, y las cookies y otras intrusiones en nuestro ordenador se las introducirá al ordenador anónimo.

Estas funciones de anonimicidad también existen para servidores de correo web y correo pop. En este último el correo lo envío como un mensaje normal, pero va a una máquina que le borra todo rastro de quién lo envía y los sustituye por un registro codificado, y desde allí se va a la dirección del destinatario o bien va a otro remailer anónimo, pudiendo llegar a pasar por varios de ellos.

Existen anonimizadores gratuitos (muy colapsados) y de pago (más ágiles), pero ante las presiones que reciben, algunos están empezando a desaparecer.

8.- Ultimas novedades.

Esto cada día va peor....

Gracias por leerme, espero que te haya entretenido y haber aportado algo a tus conocimientos.

Hubble, 8-)

(cuidado este servidor está en EEUU y allí funciona el carnivore)

Algunas páginas a visitar para empezar a protegernos y nuestros pc's

Asociación de Internautas:
http://www.internautas.org

Kriptopolis:
Sitio especializado en seguridad en español. Muy aconsejable.
http://www.kriptopolis.com

Criptonomicon:
Sitio especializado en seguridad en español. Muy aconsejable.
http://www.iec.csic.es/criptonomicon/

Para saber como va esto de internet y tener noticias:
http://www.villanos.net

Videosoft
Información sobre virus, scripts y vulnerabilidades, en castellano.
http://www.videosoft.net.uy

Virus Attack, información sobre virus, en castellano.
http://www.virusattack.com.ar

InoculateIt. Antivirus gratuito (inglés).
De Computer Asociates Inc.
http://cai.antivirus.com

Doctor WEB. Antivirus gratuito (inglés).
http://www

AVP. Antivirus. **No gratuito**
Kaspersky Antivirus, hay una versión en castellano.
http://www.avp-es.com
http://www.avp.ru

Cache Manager. Limpia cache de internet. Gratuito.
http://wettberg.home.texas.net/

ZoneAlarm. cortafuegos gratuito(en inglés).
http://www.zonelabs.com

Esafe. Cortafuegos gratuito(castellano).
http://www.esafe.com

PGP
Programa de encriptación y privacidad
http://www.pgp.com

GNUPG
Programa de encriptación y privacidad
http://www.gnupg.org/es

Buscador de verdad:
http://www.google.com

Si quieres enviarme un correo hazlo a:
Hubble@flashmail.com