El contenido de este fichero está publicado bajo una licencia Creative Commons.

La licencia bajo la que se encuentra este fichero es:

Reconocimiento-NoComercial-SinObraDerivada 2.1 España

Puede ver el texto completo de esta licencia en la siguiente dirección:

http://creativecommons.org/licenses/by-nc-nd/2.1/es/legalcode.es

Puede ver un resumen de las condiciones de la licencia en la dirección:

http://creativecommons.org/licenses/by-nc-nd/2.1/es/

Estas condiciones son:

Usted es libre de:
copiar, distribuir y comunicar públicamente la obra

Bajo las condiciones siguientes:
- Reconocimiento. Debe reconocer y citar al autor original.
- No comercial. No puede utilizar esta obra para fines comerciales.
- Sin obras derivadas. No se puede alterar, transformar o generar una obra derivada a partir de esta obra.
- Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.
- Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Los derechos derivados de usos legítimos u otras limitaciones reconocidas por ley no se ven afectados por lo anterior.

[Capítulo 6]

Seguridad física

Keyloggers

Una manera de capturar las teclas que se pulsan en un ordenador es instalando un *keylogger*. Este es un sistema que registra todas las teclas que pulsamos, de forma que, posteriormente, podrán ser leídas por el atacante, ya sea directamente en el ordenador o bien enviadas de forma remota (p.ej. por correo electrónico). De esta forma, ni tan solo es necesario el acceso físico a nuestro ordenador para obtener los datos.

Esto permite a un atacante leer todos los datos que introducimos, tales como contraseñas, números de cuenta bancaria, correos, conversaciones en chats, etc... Es evidente el alto riesgo que esto supone para nuestra seguridad y para nuestra privacidad.

Existen dos tipos de *keyloggers*:

- los basados en hardware, como por ejemplo *KeyGhost*. Estos se conectan entre el teclado y el ordenador, por lo que el atacante necesitará disponer de acceso físico a nuestro sistema, tanto para instalarlo como para recuperar los datos.

- los basados en software, como *Ghost Keylogger*, que se instalan como cualquier otro programa. Suelen incorporar muchas características, como el envío automático de los datos al atacante, la realización de capturas de pantalla a intervalos regulares,...

Detectar este tipo de programas puede resultar bastante difícil, ya que suelen utilizar técnicas para ocultarse y no ser descubiertos. Además, algunos virus y *spyware* llevan incorporados *keyloggers* para poder robar información del usuario.

Para detectar los que están basados en software podemos utilizar programas como *KL-Detector* o *Anti-Keylogger*, que se basan en detectar si algún archivo crece de forma continuada cuando pulsamos teclas. De esta forma, pueden saber si algún programa está guardando las pulsaciones que realizamos en nuestro teclado. Los *keyloggers* hardware no pueden ser detectados por software, así que necesitaremos comprobar que nuestro teclado está conectado directamente al ordenador y no con algún artilugio desconocido entre ellos.

ATENCIÓN

No siempre el uso de un *keylogger* tiene que ser perjudicial. Podemos utilizarlo como un sistema de copias de seguridad de todo aquello que escribimos, lo cual puede ser muy útil para escritores, estudiantes realizando un trabajo o cualquiera que tenga que escribir grandes cantidades de texto.
Lo importante es que seamos nosotros quienes lo hayamos instalado y seamos conscientes de que está instalado y registrando nuestra actividad.

Ordenadores portátiles

En caso de que dispongamos de un ordenador portátil deberemos tener más precauciones con él que con un ordenador de escritorio, pues este es más vulnerable.

En primer lugar, deberemos tomar las medidas adecuadas para que el ordenador no pueda ser robado. La primera medida básica para esto es no perder nunca de vista el ordenador, a no ser que esté en un lugar completamente seguro. En caso de que estemos en un lugar poco seguro, deberemos intentar alejarnos lo menos posible de él. Si estamos en algún lugar público donde sean frecuentes los robos, no deberemos soltarlo nunca, llegando, si es necesario a llevarlo colgado al cuello y cruzado, de forma que no nos lo puedan quitar por el método del tirón.

Cuando estemos trabajando con él en algún lugar público o semi-publico podemos optar por utilizar cables de seguridad, como los de tipo *Kensington*. Estos cables son de acero y permiten amarrar el portátil a la mesa, de forma que nadie podrá llevarse el ordenador, existiendo modelos que incorporan alarma para avisarnos de un intento de robo. Para ello, es necesario que el portátil disponga de la correspondiente ranura para acoplar este tipo de cables, aunque hoy en día es habitual que la mayoría lo incorporen.

Para el caso de que perdamos o nos roben el portátil será útil que hayamos realizado unas cuantas acciones preventivas, tanto para impedir el acceso a los datos por parte del ladrón como para disponer nosotros de esos datos. En primer lugar, es más que aconsejable tener activada la contraseña tanto de arranque como la del sistema operativo. Esto detendrá, como mínimo al ladrón inexperto, pero no evitará que alguien con conocimientos acceda al ordenador. Por ello la mejor opción es guardar todos nuestros datos cifrados, existiendo multitud de programas que realizan esta función e incluso algunos que vienen con el propio sistema operativo. No debemos confiar en la protección que nos puedan ofrecer los programas de ofimática (Word, Excel,...) cuando guardamos los ficheros con contraseña, ya que estas son fáciles de descubrir.

Idealmente, guardaremos también todos nuestros datos en un sistema aparte, ya sea almacenándolos externamente a través de Internet o bien mediante un disco duro USB que mantendremos alejado del ordenador cuando no estemos utilizándolo para evitar que nos roben los dos simultaneamente.

Además, debemos estar preparados para poder hacer una denuncia. Para ello, tendremos apuntado el fabricante, el modelo y el número de serie de nuestro ordenador, además de guardar copia de la factura de compra. De este modo, podremos realizar fácilmente la denuncia ante la policía y, en caso, de que el ordenador sea encontrado podremos recuperarlo mucho más rápidamente al poder aportar pruebas de que el ordenador es realmente nuestro.

Es importante realizar cuanto antes la denuncia a la policía en caso de robo, pues puede llegar a facilitar mucho la recuperación de nuestro portátil y de la información que contiene.

Seguridad en una red desconocida

Si disponemos de un portátil y nos desplazamos frecuentemente con él, es fácil que necesitemos conectarnos a la red interna del sitio donde estemos (trabajo, universidad…) Debemos tener en cuenta, en ese caso, tanto la seguridad de nuestro portátil como la de la red donde vamos a acceder.

Siempre que nos conectemos a una red desconocida o poco confiable debemos asegurarnos de tener activo nuestro cortafuegos, con todos los puertos posibles cerrados al exterior. Además, tendremos que asegurarnos que el cortafuegos está configurado para protegernos de ataques desde esta red, ya que a veces estos, por defecto, solo nos protegen de ataques procedentes de Internet. Es importante también que no tengamos activado la compartición de ficheros de Windows si no la necesitamos y, en caso de que esta sea necesaria, debemos protegerla con una buena contraseña.

Además, nunca debemos acceder a servicios inseguros (cualquiera que envíe nuestra contraseña sin cifrar a través de la red, como POP3 o FTP) cuando estemos en una red no confiable, ya que es muy sencillo para un atacante ver todos los datos que circulan por esta red. Lo mejor en estos casos será acceder solo a servicios que funcionen a través de SSL, como HTTPS o POP3 + SSL.

También es importante tener en cuenta la seguridad de la red donde accedemos. Por ello, debemos comprobar siempre que nuestro ordenador no está infectado con un virus o un gusano que pueda entrar en esta red e infectar al resto de ordenadores, además de procurar no saturar el ancho de banda disponible con transferencias de grandes ficheros si no es imprescindible, como detalle de cortesía hacia los demás usuarios de esa red.

Redes inalámbricas

Desde hace un tiempo las redes inalámbricas se están poniendo de moda debido a la facilidad de instalación de estas y la comodidad de no tener que instalar cable hasta cada uno de los ordenadores que queremos conectar.

El problema de este tipo de redes es su falta de seguridad, al estar el medio físico por el que viajan los datos al alcance de todo el mundo; es decir, cualquiera, tan solo situándose en la zona de cobertura de la red inalámbrica puede escuchar lo que se está transmitiendo. Por lo tanto, solo debemos poner nuestra tarjeta de red inalámbrica en modo *escucha* y darnos un paseo por la calle para encontrar cientos de redes inalámbricas desprotegidas y de fácil acceso.

Para solucionar este problema se propuso el estándar WEP (*Wired Equivalent Privacy*) que transmite los datos cifrados a través de la red. Pero este protocolo es demasiado débil y está mal diseñado, por lo que resulta realmente sencillo descubrir cual es la clave que se utiliza y, por tanto, acceder a la red y registrar los datos que circulan por ella. Existen incluso programas que lo hacen de forma automática y muy sencilla, como Airsnort.

Por ello, se han propuesto otros protocolos como WPA (*Wi-Fi Protected Access*) que mejoran la seguridad de WEP, aunque tampoco son infalibles. Es por ello que debemos tomar una serie de precauciones al instalar una red inalámbrica:

- Activar siempre el protocolo WPA o, en su defecto, el protocolo WEP. Aunque estos sean débiles es mejor tenerlos activados para dificultar la tarea a un posible atacante.

- Activar el filtrado por MAC (la dirección física de la tarjeta de red inalámbrica), de forma que solo puedan conectarse al punto de acceso aquellas tarjetas a las que nosotros demos permiso.

- Usar un sistema de autenticación, como NoCatAuth.

- Usar antenas que emitan solo en la dirección que nos interesa.

- A ser posible, separar completamente la red inalámbrica del resto de la red. Instalar un cortafuegos y dar permiso solo a aquello que necesitemos.

ATENCIÓN

El desarrollo de la banda ancha y las tecnologías inalámbricas han propiciado la aparición de comunidades conectadas a través de este tipo redes, a veces ofreciendo servicios propios y otras simplemente conexión a Internet.
Si nos interesa el tema podemos ponernos en contacto con la comunidad de nuestra ciudad, donde nos informarán oportunamente.

Algunos ejemplos de estas comunidades:

http://www.barcelonawireless.net
http://www.madridwireless.net
http://www.zaragozawireless.org

Referencias

Keylogger basado en hardware
http://www.keyghost.com/

Keylogger basado en software
http://www.keylogger.net/

Dirección de descarga de KL-Detector
http://dewasoft.com/privacy/kldetector.htm

Dirección de descarga de AntiKeylogger
http://www.anti-keylogger.net/