¿Y si me afanan el ordenador portatil?

Un ordenador portátil de un empleado de BP fue robado contiendo información confidencial sobre 13.000 personas que reclamaron compensaciones tras el vertido de petróleo en el Golfo de México. A pesar de que tenía una contraseña, la información de los ciudadanos afectados no estaba encriptada por lo que permanece expuesta a filtraciones.

Cada vez más gente tenemos un ordenador portátil y ciertamente casi nadie asume que su ordenador puede ser robado o perdido, por lo que raramente tomamos precauciones para evitar las consecuencias de la sustracción. ¿Y por qué me iba a tener que pasar a mí? Si así sucediera, lo peor, con ser bastante, no sería la perdida de datos almacenados en la máquina y que habría que recuperar en el supuesto de tener copia de seguridad en algún lugar, sino que esos datos pasen a manos ajenas con las implicaciones que ello pudiera tener. Documentos personales o corporativos, fotos, códigos, contraseñas, ¿hay que seguir con la lista? pueden ser usados por el ladrón de forma fraudulenta. Quizá por desconocimiento o por desidia o porque pienso que a mí no me lo van a robar, casi nadie protege el ordenador portátil para estas eventualidades.

Lo mínimo que habría que hacer es configurar el ordenador para obligar al usuario a facilitar una contraseña para poder conectarse a él. Si la contraseña es lo suficientemente robusta no será fácil de descubrir e impediría en principio el acceso a la máquina y por tanto el acceso a los datos. ¿Pero y si los ladrones retiran físicamente el disco y se lo llevan a otra máquina? Es un trabajo sin dificultad que permitiría acceder alegremente a todo el disco a pesar de la contraseña.

Si en algún lugar de ese disco a su vez hubiéramos guardado las contraseñas de correo electrónico, de comercio *online*, de entidades financieras... sin comentarios. En estas circunstancias nos vendría muy bien, es obligado diría yo, un gestor de contraseñas para tenerlas todas ocultas. Existen gestores que las ocultan en el ordenador o en un servidor web accesible por internet.

Pero si realmente lo que pretendemos es que el disco quede protegido en caso de robo, habrá que tomar otras medidas como, por ejemplo, que trabaje con los datos encriptados, o cuando menos, con aquellos datos que consideremos críticos. Ello impediría su lectura a terceros en caso de robo. La encriptación de los datos podría ser reemplazada con el depósito de estos «en la nube», si ello nos merece confianza, lo que nos evitaría tenerlos en el disco del ordenador.

Con lo hasta aquí hablado, si nos roban, nos hemos quedado sin máquina, pero al menos no nos han leído los datos. Existe también la posibilidad de seguir el rastro a través de Internet a la máquina robada mediante un software adecuado y con ciertas limitaciones. Para ello, es obviamente imprescindible que el ordenador sustraído sea puesto en marcha y conectado a Internet. Los programas de rastreo se valen de técnicas diversas y dan ubicaciones aproximadas de donde pudiera encontrarse, pero al final debería ser la policía quien lo recuperara.

En el cuadro adjunto se exponen algunos de los programas (hay muchos más), varios de ellos gratuitos, que pueden auxiliarnos para implementar las diversas medidas de seguridad aquí propuestas, dejando al criterio del lector qué iniciativas tomar para proteger su ordenador portátil si teme la pérdida o el robo.

Jesús Sanz

Software de protección

Gestor de contraseñas:

KeePass. Todas las contraseñas son encriptadas y bloqueadas por una contraseña maestra que es la única que hay que recordar. Gratuito.

Cifrado de contenidos:

TrueCrypt. Encriptador de datos en el disco permitiendo crear un volumen virtual de forma automática y transparente. Gratuito.

Software de recuperación:

Adeona Rastrea la ubicación del ordenador usando la dirección IP en caso de extravio o sustracción y encripta los datos. Gratuito.

Prey. Usa el GPS del dispositivo o puntos de acceso Wifi próximos a él para obtener la ubicación. Permite bloquear la máquina impidiendo su uso. Gratuito.

LocatePC Transmite con regularidad por *email* la dirección IP a la que está conectado. Puede grabar y transmitir la imagen de la persona que lo está usando.

LoJack En caso de aviso de robo, rastreo y localización por un centro de control, utilizando Internet. Permite eliminar la información de forma remota.

Reconocimiento facial:

El sistema de reconocimiento facial escanea el rostro del usuario permitiendo su identificación para autorizar el acceso al ordenador. Funciona en ciertas máquinas de HP.