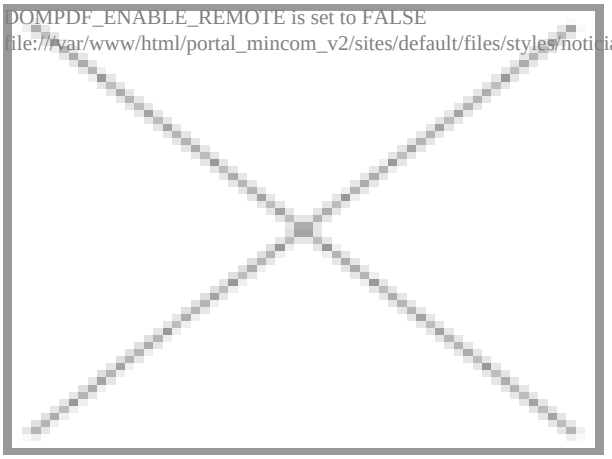

Source:
Diario TI

Opinión: El robo de 68 millones de cuentas en una de las nubes más famosas de la red, Dropbox, ha vuelto a poner, una vez más, en tela de juicio su seguridad.

Continuamente personas y empresas comparten información a través de la red o, simplemente, la almacenan. Archivos en forma de imágenes o documentos, más o menos confidenciales, que viajan todos los días de un lugar a otro, de una persona a otra, quedándose en uno o varios dispositivos, aunque no siempre de manera segura.

Son muchas las formas de almacenar y transferir documentos que existen, pero una de las más cómodas, accesibles y sencillas de utilizar es la nube pública. Cada vez son más personas las que las usan y, también, las que desconfían de ellas.

El robo de 68 millones de cuentas en una de las nubes más famosas de la red, Dropbox, ha vuelto a poner, una vez más, en tela de juicio su seguridad. El servicio de almacenamiento advirtió a todas aquellas personas que tuvieran una cuenta abierta antes de 2012 que cambiaran su claves de acceso, además de en aquellas redes o sistemas en los que fuera la misma contraseña para evitar poner en peligro más información.

Imágenes comprometidas de miles de mujeres famosas robadas en iCloud o filtrado de nombres e informaciones confidenciales en los Papeles de Panamá, Dropbox es tan solo el último caso de una larga lista de hackeo masivo de archivos en nubes públicas. Así es como las nubes públicas se han ganado la etiqueta de inseguras, algo que no tiene por qué ser siempre así.

Si los archivos hubieran estado totalmente protegidos, ni si quiera el mejor hacker del mundo habría podido descifrarlos. A través de un servicio de encriptación, se crea una segunda capa de protección adicional sobre cada fichero, sea del tipo que sea, de manera que solamente el propio usuario es capaz de acceder a él y dar los permisos que elija a terceros.

Si un hacker consigue penetrar en el archivo, las soluciones IRM permiten al usuario ver quién accede, de qué forma o cuándo lo hace, teniendo la opción de destruirlo de forma remota en cualquier momento y lugar, de manera que solamente él es el que puede acceder.

Una inseguridad que se puede transformar en tranquilidad si se tiene el control de todos los ficheros que se almacenan y comparten a través de nubes públicas, impidiendo a los hackers darles vía libre para acceder a lo que es nuestro, esté en Dropbox o en cualquier otro servicio.

Disponible en:

http://diarioti.com/las-nubes-publicas-no-tienen-por-que-ser-inseguras/100360 [1]

Links
[1] http://diarioti.com/las-nubes-publicas-no-tienen-por-que-ser-inseguras/100360