Asociación de Internautas

Hacking RGPD.

¿Cuántas veces te ha pasado que se te ha roto un disco duro, una tarjeta de memoria, te has cambiado de tablet o de móvil? A dia de hoy, es lo más común del mundo. Pero, ¿has extraído o destruido la unidad de almacenamiento? La mayoría de las veces, no se hace porque somos demasiado confiados, pero la realidad resulta escalofriante: todo aquel que encuentra un dispositivo de almacenamiento, lo prueba en un ordenador a ver qué lleva; que tú no puedas acceder no significa que otro no pueda.

Que levante la mano aquel que se ha encontrado un Pen Drive en la calle y se lo ha llevado a su casa "a ver qué contiene". Esa práctica puede resultar una imprudencia, pues hoy día se puede hackear un PC con meter un simple Pen Drive en un USB, no es la finalidad de este artículo cómo se puede hacer esto, pero prometo hacer otro al respecto.

Caso 1. El confiado.

Hace unos 7 años compré una tablet de la marca Siroco, no estaba mal para aquel momento pero en cuanto Android cambió de versión, bien podía usarse como soporte para cortar tomates. Desesperado, la abandoné en un cajón y allí estuvo hasta que hice la mudanza para cambiarme de piso, y mi forma de proceder fue la más normal del mundo: saqué la microSD (reutilizable con mis IoT) y la tiré, junto con mil cachivaches más, a un contenedor de reciclaje.

Unos dos meses más tarde, Google me enviaba un correo de inicio de sesión desde Casablanca (Marruecos). Y supe con total seguridad que era aquella Tablet, pues ninguno de mis móviles lo he tirado (se los dejo a los clientes que necesitan uno de sustitución, configurándolos con sus cuentas). Por supuesto, tocaba cambiar claves de acceso a la cuenta implicada, y a preguntarme qué información quedaría en el dispositivo (no demasiada pues la usaba para leer mis novelas frikis)

Caso 2. La ingenua.

Una amiga tenía un portátil "del año de la Polca", es decir, pantalla 4:3, disco de 30 Gb, 512 Mb de memoria, grosor de ladrillo termoaislante… Pero curiosamente, funcionaba bastante bien con XP. Me llama para decirme que lo quiere donar a Cáritas, y le digo que es necesario limpiárselo antes. Me comenta que "ya ha tirado y vaciado la papelera", pero de todas formas, me lo deja y justo antes de borrar concienzudamente el disco duro, me da por probar hacerle una recuperación de datos. Salieron hasta las fotos del bautizo de su hija (tiene ya 20 años la criatura), recetas de cocina, cartas de amor de un romance lejano… Le hago un borrado en condiciones, eliminando XP, vuelvo a comprobar la recuperación de datos y, siendo completamente negativa, le meto Xubuntu (una versión de Linux muy muy ligera), y lo lleva a Cáritas. Cero problemas. Me puedo imaginar a su destinatario actual haciendo lo imposible para recuperar algo de su anterior propietario, ofuscándose en el intento (jaja, mis métodos de borrado se perfeccionan con el tiempo).

Caso 3. Hacking RGPD.

Cliente que me llama, muy apurado: se le ha desaparecido una carpeta importantísima que tenía en el escritorio de su ordenador, y sabe que hago magia (milagros, no; magia, sí). Mi primera opción es buscarla empleando los recursos del sistema operativo… nada. Miro el disco, sólo tiene ocupado unos 80 Gb, de 1 Tb de disco (Windows 7, Office 2007 y lo que tenga de documentos; por la cuenta de la vieja, sale) y le digo que me lo voy a llevar, que es tarde (es demasiado frecuente volver de «hacer la calle» a las tantas), y que mañana se lo traigo. Llego a mi Santuario (ejem, mi despacho), desarmo el equipo, enchufo el disco duro en un PC especial que tengo para ello, y procedo a realizar una extracción de información. El disco se pone a girar y al rato, al ver que no termina, lo dejo funcionando y me voy al sobre (gracias a Dios, está lo suficientemente cerca para ir casi con los ojos cerrados).

Por la mañana, 7 horas más tarde, veo que sigue trabajando el equipo. Va por el 80%, me susurra la pantalla; extrañado, llamo al cliente y me dice que compró el equipo hace 2 semanas en una tienda de segunda mano, una torre i5 con 4 Gb por 250 euros. Le pido que me envíe un correo con el contenido que recuerda que tiene, porque me temo lo peor, que tenga que rastrear todo el contenido, y una copia de la factura (milagrosamente, la tiene; veo que se lo venden sin garantía). Termina a eso de las 16:00 horas, y no sólo encuentra lo que el cliente me ha pedido que le busque, sino con millones de cosas más: fotos, vídeos, documentos de texto, hojas de cálculo, bases de datos, pdf… Algunos ficheros han sido pisados por otros, pero la mayoría son recuperables, unos 800 Gb.

Comienza el terror (*)

Archivos con datos de acceso a correos electrónicos, servidores, contraseñas, herencias, declaraciones de la renta, base de datos con datos personales, fotos de viajes, de eventos, de … Cosas “innombrables”. Sé que no son de mi cliente porque 800 Gb de información no son los 80 Gb ocupados. Algunos archivos no tienen fecha, no tengo metadatos para poder localizarlos en el tiempo, pero otro sí, desde hace años hasta hace un mes. Empieza lo más tedioso, encontrar los de mi cliente, que voy almacenando en un disco externo nuevo. Pero… mientras, va apareciendo evidencias de un pasado tenebroso de la información que ha contenido ese disco.

¿De quién era ese disco duro?

¿De quién es propiedad ahora esos datos?

Porque mi cliente HA COMPRADO EL EQUIPO y, con él, la licencia del sistema operativo y de los programas que contuviese, así como la información que se encuentre en el disco duro. *¿También es dueño de su pasado?*

¿Se está vulnerando el RGPD? Porque toda esta información es de alguien y lo que es peor, si se analiza, hay hechos delictivos en ella.

¿Quién tiene la responsabilidad del no haber realizado correctamente el borrado? ¿Quién lo vende? ¿Quién lo compra? ¿El intermediario?

Sé que, como Perito Judicial Informático Forense, cuando realizo una pericial, debo atenerme a los hechos tal cual me los solicita el cliente o el juzgado, además de hacerles firmar un documento de confidencialidad a las partes implicadas de no revelación de la información obtenida; pero este caso presenta una especial complicación, ya que además de los datos de mi cliente, existen otros que, en una situación anómala y más frecuente de lo común, podrían incriminarlo en uno o varios delitos si

no se tomaran las medidas oportunas.

En aras de librarlo de una preocupación mayor, lo llamo y le digo que el disco presenta un fallo mecánico, que hace que la información se pierda, «posiblemente se haya desmagnetizado, de ahí su precio» (mentirijilla piadosa que lo exonera de toda culpa). Le hablo de adquirir un disco duro nuevo, en formato SSD (disco sólido, para quien no está familiarizado, van 10 veces más rápidos que los discos electromagnéticos), con el que el equipo «volará», podrá mantener las licencias de Windows y de Office contenidas en el disco viejo, pero con que la mano de obra de instalación de todo y de la recuperación de la información, prácticamente le habría salido más económico haber(me) adquirido una torre nueva, con sus 2 años de garantía y sin usar. Se lo envío por escrito, me da el visto bueno y al día siguiente la tiene funcionando en su oficina.

Siguiente paso, ponerme en contacto con las FCSE y hacerles llegar la evidencia. No hay problema, no es una prueba, pero sí es una pista. El anterior dueño del equipo estará haciendo lo mismo, nadie cambia de vida cuando sustituye su ordenador, al contrario: más rápido, con más almacenamiento, más puede guardar. Ya sabes a quien dirigirte (en este mundo, siempre conoces a alguien, magistrados, fiscales, abogados… incluso GC y PN), pero llamas a varias puertas para que te indiquen el camino correcto. Se entrega, haces lo que debes hacer, como profesional, como ciudadano, al servicio de tu país. Y no esperas nada a cambio, a lo sumo, te consultan en el futuro sobre cómo proceder, si te ven a menudo aquí y allá. A veces coincides en algún evento, en un control rutinario (me ha pasado), y no hay más tranquilidad en tu alma que saber que ayudas. Y ellos saben que no eres uno más, sino que estás ahí para lo que necesiten (sentimiento importante a tener en cuenta: también son personas). En nuestro código deontológico, los Peritos Judiciales Informáticos Forenses debemos prestar nuestro conocimiento, sapiencia y experiencia a las FCSE cuando lo necesiten. Incluso se le hace entrega del informe forense, que es un escrito donde se detallan las técnicas utilizadas, las aplicaciones forenses empleadas y se detallan los hechos tal y como se conocen y han ocurrido.

Conclusiones

Siempre que vayas a dejar de utilizar la tecnología por otra mejor, elimina o destruye físicamente el contenido. Si lo vas a vender, asegúrate que no es accesible, contrata a un profesional que te lo destruya (aviso: barato no es, pero si es buen profesional se limitará a borrarlo).

Un disco duro hay muchas formas de eliminar su contenido. Si no se va a volver a utilizar, se desmagnetiza y se destruye, como las pulverizadoras de discos duros que veis en las fotos. Yo prefiero desmontarlos y con los platos cerámicos que almacenan la información, construyo colectores solares (un ciberingeniero eléctrico friki es lo que os faltaba por ver; otro día hablaré de ellos, jaja.)

Sé que el negocio de revender equipos usados da muchos beneficios: prácticamente te los regalan, aprovechas la licencia, borras lo que haya y lo vendes tirado de precio para que te los quiten de las manos… Pero no hacer ese proceso correctamente puede dar lugar a casos como el que he descrito y que, en un momento dado, quien vende el equipo puede ser responsable civil (o penal) de su información contenida, aunque no sea visible (por eso solicité la factura, práctica que debéis hacer siempre con cualquier material tecnológico que adquiráis), y que alguien te venda un equipo con información comprometida… Es para pensárselo.

*Sólo me queda hacer constar que “cualquier parecido con la realidad es pura coincidencia”.

Artículo de Alejandro Cortés, Cryptodeveloper & CiberForense en Jenhyal S.L., publicado en Derecho de la Red