

Última

La informática forense, a la caza del empleado traidor

Alfonso Simón / MADRID (03-07-2007)

Publicado en: Edición Impresa - Empresas

El director comercial de una gran consultora se despide de su empresa. Al día siguiente se marcha el director de producto. A los tres días se empieza a ir una parte importante de los empleados de la compañía. Los jefes no entienden qué ocurre, pero sospechan que es una trama para marcharse a la competencia. Por ello contactan con Incide, la rama digital de la agencia de investigadores privados Winterman. Temen que en la salida de sus directivos haya un caso de competencia desleal y fuga de información. Los detectives buscan rastros en los ordenadores de los directivos y efectivamente encuentran indicios de una salida organizada a la competencia.

Este es un caso real para la informática forense, que mediante informes periciales describe posibles delitos. Para las empresas, la marcha de directivos puede ser una muy importante fuga de información de forma ilegal. El enemigo está dentro, según explica Abraham Pasamar, director de Incide: 'El mayor número de incidentes de seguridad, más del 80%, son internos'. Éstos suelen ser la fuga de información, los accesos a recursos no autorizados, la intrusión en el correo electrónico, la competencia desleal o el sabotaje informático.

¿Cómo probar estos delitos? Los peritos informáticos se acercan a la empresa, normalmente acompañados de un notario y una cámara fotográfica, y, sin alterar nada, realizan una copia perfecta del disco duro, llamada copia espejo, manteniendo una cadena de custodia segura de la información. Una vez en el laboratorio trabajan con la copia para buscar las huellas del delito. En el anterior ejemplo de competencia desleal, se realizó una búsqueda de palabras clave que relacionasen a los ejecutivos con la marcha a otra empresa con información clave. Los rastros aparecieron en las cuentas personales de Yahoo.

Del disco duro no se puede leer todo ni abrir cualquier archivo, ya que -respetando la intimidad de las comunicaciones- los indicios deben de ser buscados dentro de la legalidad. El paso final para el investigador es la elaboración de un informe pericial que servirá de prueba en posibles juicios. El coste medio del trabajo ronda los 3.000 euros, según la empresa catalana Incide.

El trabajo de los peritos se convierte en fundamental para los abogados que defienden a las empresas. 'Hay veces que el informe que nosotros elaboramos es todo el caso', cuenta Juan Martos, director de laboratorio de la empresa española Recovery Labs, especialista en recuperar información de los discos duros.

'El mayor número de incidentes en la seguridad, más del 80%, son internos', explica el director de Incide, la rama digital de una compañía de detectives

Y es que un ex empleado puede hacer mucho daño. Martos explica que los sabotajes son una parte sustancial de los casos en los que ejerce como perito. Relata cómo en una ocasión un director de sistemas que había sido despedido destruyó una gran cantidad de información del servidor de su antigua compañía. Ahí entró en acción Recovery Labs. Averiguaron el día en el que se produjo el borrado y descubrieron que se había realizado desde la casa del que fuera ejecutivo de la empresa.

Pasamar advierte de la importancia de prevenir la destrucción o la fuga de información. Actualmente existen programas que marcan como seguros archivos importantes y si se mueven o se modifican provocan una alerta.