

ROSARIO SEPÚLVEDA

Resentidos, despedido como los amantes. El sentimiento de ira que provoca la comunicación de un despido no dista mucho del que produce el conocimiento de cualquier noticia traumática. «Se han descrito cinco fases en estos procesos: negación, ira, negociación, depresión y aceptación. De ahí que, al enterarte que te han despedido, lo ideal es alejarte de la empresa sin actuar ni comprometerte a nada. Intenta mantener la sangre fría, porque todas las reacciones que brotan de un 'calentón' son erróneas. Ya habrá tiempo después, incluso, para perdonar», aconseja el psicólogo Marcos Chicot, autor del libro '¡Me han despedido!', publicado por Plataforma Editorial.

Sin embargo, no todo el mundo termina por aceptar el trago de verse en la calle y, acomodados en ese sentimiento de ira sobre el que alerta Chicot, urden o improvisan una venganza contra su antigua empresa. «Cada vez hay más casos en los que los sistemas de información y los datos de las compañías son objeto de robo o manipulación por parte de los ex empleados», confirma Marc Martínez, socio del área de Información Technology Risk Advisory de Ernst & Young, que acaba de publicar el informe '2009 Global Information Security Survey'.

Basado en entrevistas a ejecutivos de 1.900 organizaciones de 60 países, el estudio desvela que las represalias por parte de antiguos empleados, así como la escasez de presupuesto para acometer un buen plan de seguridad, suponen los mayores quebraderos de cabeza de los directivos que gestionan la seguridad de la información en las empresas.

### Aumento del 60%

El Gabinete Profesional de Peritos Judiciales también advierte un aumento exponencial de sabotajes informáticos como respuesta al despido desde que empezó la crisis. Manel Cruz, su gerente, estima que, en el último año, han cursado el 60% más de estos casos. «Lo más habitual es sacar información de la compañía o borrarla. El mes pasado, por ejemplo, un ex empleado de un estudio de arquitectura sacó de allí planos que no le pertenecían, porque eran propiedad intelectual de la empresa. En el 80% o 90% de las ocasiones, sin embargo, la información borrada se recupera, siempre y cuando la máquina no se haya tocado tras el sabotaje».

Ernst & Young acaba de inaugurar un laboratorio de

# La venganza de los 'ex'

## Con la recesión económica han crecido las represalias de los empleados despedidos contra sus empresas



Los sabotajes informáticos incluyen el robo, la manipulación y el borrado de información. :: CHRIS HONDROS-AFP

tecnología forense en Madrid que permite recuperar esa información al tiempo que encontrar las evidencias de comportamientos desleales por parte de los trabajadores.

La forma de la venganza puede ser tan variada como los motivos que subyacen tras ese comportamiento. En algunos casos, como en la venta de datos, patentes o diseños a la competencia o el robo de la cartera de clientes para emprender en solitario, el despedido busca lucrarse; en otros, sin embargo, se comporta como un animal herido que sólo quiere hacer daño. En este epígrafe se encuadran las denuncias por incumplimiento de la Ley de Protección de Datos, que acaban saldándose con multas para la empresa, y las denuncias contra pymes por el uso de 'software' ilegal. Estas dos formas de revancha han crecido en los últimos años.

Con la proliferación de sencillos dispositivos electrónicos con capacidad para grabar grandes volúmenes de datos y el deficiente control sobre su información crítica —todo ello sin contar con las sofisticadas técnicas de los 'ciberespías'—, las empresas están cada día más expuestas a las represalias de sus 'ex'.

Uno de los datos más llamativos del estudio de Ernst

& Young es el relativo a las pocas empresas que cifran sus ordenadores portátiles, sólo el 41% lo hace. El bajo porcentaje sorprende tanto por el creciente número de incidentes derivados de la pérdida o robo de portátiles como por la gran variedad de tecnologías que combaten estos percances a muy bajo precio. «En primer lugar, las organizaciones tienen que decidir qué es infor-

### Los despedido suelen recurrir a los sabotajes informáticos

### Sólo cuatro de cada diez empresas cifran sus ordenadores portátiles

mación crítica y, en torno a ella, establecer las medidas de control oportunas para reducir los riesgos que conlleva su exposición», apunta Marc Martínez.

### Medidas de control

Prevención, prevención, prevención. Ésta es la consigna de José Manuel Rodríguez, abogado de CMS Albiñana & Suárez de Lezo, para evitar las

fugas de información. El abogado recomienda, por ejemplo, introducir cláusulas de confidencialidad en los contratos, restringir el acceso de los trabajadores a según qué información, redactar códigos de conducta donde se advierte y explique qué puede ser causa de despido, anular todos los accesos al sistema ('webmail...') y a la propia empresa desde que el despido es comunicado e, incluso, incorporar medidas de vigilancia y control de la plantilla, sin vulnerar, eso sí, el Estatuto de los Trabajadores. «El trabajador tiene que estar advertido previamente. Pero hay una sentencia del Tribunal Supremo del 2007 que ampara la monitorización de las computadoras. Hasta entonces, los ordenadores en España se equiparaban a las taquillas», explica Rodríguez.

Dada su renuencia para invertir en seguridad, las empresas pueden terminar pagando caro sus descuidos. Por ejemplo, ante los casos de empleados que utilizan información corporativa para enriquecerse con una actividad paralela, Marc Martínez afirma que es mucho más fácil demostrar el delito cuando el profesional está dentro de la empresa —«porque la gente es poco cuidadosa y no sabe el rastro que deja. Se pueden reconstruir los archivos de varios meses sin que el investigado lo sepa»— que una vez fuera. Tampoco son fáciles de demostrar los robos de clientes o de estrategias de negocio. «Muchas empresas se han querrellado contra antiguos empleados que se lo han montado por su cuenta —añade José Manuel Rodríguez—. Pero pocas veces el Tribunal de Defensa de la Competencia ha fallado a su favor. Y entiendo que así sea. Existen cláusulas de no competencia en los contratos de trabajo; pero, además de que han de ser remuneradas, tienen un límite de dos años».

## Cómo reforzar la frontera entre el 'usuario' y la 'contraseña'

R. S.

Usuario y contraseña. Ésta suele ser la única frontera que separa la información de una empresa de sus potenciales usuarios. Pero, dado que se trata de una precaución demasiado genérica, a veces no es suficiente. La gestión de identidades, que permite controlar los permisos de acceso de cada empleado a los sistemas corporativos, va un poco más allá.

También aportan garantías adicionales de seguridad los certificados digitales, que incluyen una tarjeta con chip. «Esto se puede



MAURICIO ASCIONE

complementar con algún tipo de información biométrica, que añade al certificado el control de la huella. Cada vez se emplean más este tipo de soluciones, sobre todo en entidades financieras», afirma Marc Martínez, socio del área de Tecnología Risk Advisory de Ernst & Young. La firma de servicios profesionales dispone de un laboratorio de simulación que permite adelantarse y, por tanto, prevenir los riesgos de un ataque externo. «Son servicios muy demandados por los clientes para evitar es-

pionajes informáticos», asegura Martínez.

Por lo que respecta a los sistemas de blindaje con que las organizaciones pueden proteger su información crítica, es posible, por ejemplo, implantar políticas de seguridad que eviten la copia de documentos a soportes CD o DVD o, incluso, impedir su envío por correo electrónico.

El estudio '2009 Global Information Security Survey' pone de manifiesto que «el nivel de riesgo, tanto interno como externo, sigue aumentando». De ahí que el 40% de los directivos consultados se haya fijado como segunda prioridad para los próximos meses implantar o mejorar las tecnologías de fuga de datos (Data Leakage Prevention- DLP).