

Pocas organizaciones inscriben sus ficheros en la Agencia de Protección de Datos

La sustracción de información en España es cada vez más frecuente - El motivo del robo es obtener datos de la competencia - La ley española castiga hasta con 600.000 euros la pérdida de datos médicos

MERCÉ MOLIST

EL PAÍS - 23-06-2005

El último caso, esta misma semana. Un pirata informático ha puesto en peligro los datos personales y bancarios de los titulares de 40 millones de tarjetas de crédito de entidades financieras como MasterCard, Visa o American Express. Hace dos semanas, Citibank perdía los datos de 3,9 millones de clientes. Desde principios de año, importantes empresas de EE UU han perdido o les han robado bases de datos con información de millones de personas.

Lo que a primera vista parece una oleada es, según los expertos, algo normal. La diferencia está en que nadie lo denunciaba, hasta la aparición de una ley en California que obliga a las empresas que sufran fugas a darlo a conocer públicamente.

A raíz de su entrada en vigor a mediados de 2004, empezó una avalancha de notificaciones de robos y pérdidas de datos que ha sacudido a la opinión pública y ha provocado que el Congreso norteamericano estudie poner en marcha leyes para todo el país.

Los casos destapados muestran que la mayoría de empresas ven comprometidas sus bases de datos de tres formas: por la pérdida de discos de *back-up*, que suele gestionar una tercera empresa, por la entrada de intrusos o los empleados en el sistemas informático, y por el robo de ordenadores.

La desaparición de *back-up* ha afectado al Bank of America, que en febrero perdió información de 1,2 millones de personas; al programa gubernamental Smart Pay, con más de un millón de clientes afectados; a Ameritrade, que perdió en abril los datos de 200.000 clientes, y a Time Warner, cuyas cintas de *back-up* con datos de 600.000 empleados volaron en mayo, durante un transporte.

En cuanto a la entrada en sistemas informáticos, el Bank of America es protagonista del mayor robo de datos bancarios. A finales de mayo se supo que empleados del banco vendieron información de 670.000 clientes.

En febrero, diversas personas se hicieron pasar por clientes de Choice Point para entrar en sus sistemas y robar nombres, direcciones, números de Seguridad Social e informes financieros de 140.000 usuarios. En marzo, se descubría que habían usado el mismo truco con Seisint, una filial de Lexis Nexis, para llevarse datos de 310.000 personas. El mismo mes, la empresa de calzado DSW notificaba que les habían robado los números y nombres asociados a 1,5 millones de tarjetas de crédito.

En cuanto al robo de ordenadores, la semana pasada desaparecía un portátil de MCI con información personal de 16.500 empleados. En abril, robaban dos máquinas del San José Medical Group, con información médica y financiera de 185.000 pacientes. En marzo, un contratista del Gobierno, Science Applications International Corp, sufría el robo de varios PC con detalles sobre empleados actuales y pasados, entre ellos secretarios de Defensa y directivos de la CIA.

La situación no es nueva. Tampoco es un fenómeno exclusivo de Estados Unidos. Simplemente, por ley, en ese país se obliga a declarar el extravío de datos *sensibles*.

Estados Unidos siempre ha destacado por su legislación permisiva en protección de datos, que empieza a cambiar para acercarse a la normativa europea, más proteccionista. Esta laxitud sería la explicación del desbarajuste en sus bases de datos. Pero los expertos consultados por *Ciberp@ís* sostienen que la situación no es mejor en España, sólo que aquí las empresas no están obligadas a hacer públicas las fugas.

En Europa, el caso más sonado es el del Banco Central de Rusia, al que en cuatro meses le han robado dos veces las bases de datos con las operaciones de los últimos dos años. Luego se venden en el mercado negro por 3.000 rublos (85 euros). En España, el caso más reciente ha sido el hospital de Leganés, que estos días se somete a una auditoría informática, después de detectarse "accesos atípicos".

Para Daniel Cruz, responsable del Departamento de Planificación de Seguridad de ESCERT / Inet Secur, "los robos de datos con información personal suceden también en España, donde

siempre ha existido un mercado de datos. Muchas veces no son robos de terceros, sino que las fugas provienen de la propia organización, por errores voluntarios o no".

El motivo de estos robos, cada vez más frecuentes según Cruz, suele ser "obtener datos de los clientes de la competencia". Albert Gabás, gerente de Astabis Data Management y miembro del Chaos Computer Club, explica: "Las bases de datos españolas no son más seguras que las americanas. Aquí siempre se ha pagado a *crackers* para obtenerlas: en su día daban bastantes millones por la base de datos de una importante operadora de móviles".

El peligro de las webs porno

Gabás recuerda que "casi toda intrusión en un sistema lleva asociado el acceso a la base de datos de usuarios y contraseñas. Las *webs* de sexo son uno de los principales objetivos, porque tienen succulentas listas de tarjetas de crédito y poca seguridad".

Mariano José Benito, director del Departamento de Seguridad de SGI Soluciones Globales Internet, explica: "Al no ser denunciados, no hay estadísticas fiables de estos robos en España, pero la sensación general es que hay incidentes de este tipo con cierta frecuencia y que han ocurrido en buen número de compañías de todos los sectores, desde grandes empresas hasta las *pymes*".

Benito agrega: "El origen son *spammers*, la competencia e incluso mafias, muy a menudo transnacionales. Se conocen casos de intentos de estafa basados en datos financieros de un fichero robado".

La Ley Orgánica de Protección de Datos (LOPD) española es considerada una de las más estrictas del mundo. "Hemos investigado pérdidas de bases de datos durante un transporte, su aparición en la vía pública, robos de un ex socio o empleado, en entidades financieras, hospitales, empresas y administraciones", relata Jesús Rubí, adjunto al director de la Agencia de Protección de Datos. Las multas son ejemplares: entre 60.000 y 300.000 euros, por no tener medidas de protección, y entre 300.000 y 600.000 euros por pérdida de datos de nivel alto, como la información médica.

Rubí agrega: "Hay un conocimiento creciente de la normativa. Las grandes corporaciones, que tienen las bases de datos más grandes y complejas, ya cuentan con políticas al respecto". El problema, dice, son las *pymes* y los pequeños y medianos ayuntamientos.

"En la mayoría de *pymes* no desconfían de sus empleados ni de los informáticos externos, muchas veces sin contrato ni cláusulas de confidencialidad", dice Albert Gabás. "Permiten que todos puedan acceder a todo y no hay ningún control. Pocas cumplen la ley".

"El cumplimiento de la LOPD es escaso", afirma Cruz. "El porcentaje de organizaciones que tienen inscritos sus ficheros en la Agencia de Protección de Datos no supera el 10% y la inscripción es la fase más sencilla". El portavoz de la agencia afirma que hay registrados 600.000 bases de datos de empresas, pero no puede cuantificar el porcentaje que supone, aunque sí lo califica de "bajo". "En cuanto al Reglamento de Medidas de Seguridad", sigue Cruz, "su implantación tampoco es alta porque, en el caso de ficheros de nivel alto, el proceso es complicado y costoso para las pequeñas empresas".

Datos sensibles

Benito añade: "Los hospitales, compañías de seguros médicos, sindicatos, partidos políticos, agrupaciones religiosas, tienen en su poder datos del nivel más alto, que requieren medidas de protección muy estrictas y caras. La tentación está ahí. En el sector de la sanidad no tengo constancia de incumplimiento. En el caso de las *pymes* suele deberse a desconocimiento".

El problema, continúa explicando Benito, no es que la normativa sea complicada, sino que "la complicación está en la propia organización: en muchos casos no queda claro quién se encarga de qué, en otros las tareas se interfieren entre sí". De todos modos, dice que la tendencia es positiva.

Otro caballo de batalla es la cesión de datos entre empresas, donde en algunos casos se intenta abusar, explica: "La cesión sucesiva de datos entre organizaciones hacen que un ciudadano no pueda saber cómo una entidad desconocida para él tiene sus datos. Además, hay pequeñas empresas que dan a sus clientes la falsa confianza de cumplir la ley cuando sólo lo hacen legalmente, pero no desde el control tecnológico".

Cruz critica que la normativa vigente no garantiza la confidencialidad de las bases de datos: "Es fundamental el cifrado de toda la información, en cualquiera de las etapas del ciclo, desde su entrada, pasando por el almacenamiento y transporte". El reglamento actual sólo exige cifrado en el transporte de información de nivel alto.

El Computer Security Institute realizó el año pasado una encuesta entre 276 compañías de Estados Unidos para saber por qué no denunciaban los robos en sus bases de datos: el 51% no lo hacía para no crearse mala publicidad; el 35% por miedo a que la competencia se aprovechara

del incidente; el 20% porque un remedio interno les parece la mejor opción, y el 18% por desconocimiento del interés de las fuerzas de la ley en estos casos.