

SOFTWARE ANTIFRAUDE

Un detective en la PC

Cómo son los sistemas para detectar lavado de dinero, sobrefacturación en prepagas, llamadas hechas desde un celular robado, la falsificación de un medicamento o la intrusión en una casilla de mail.

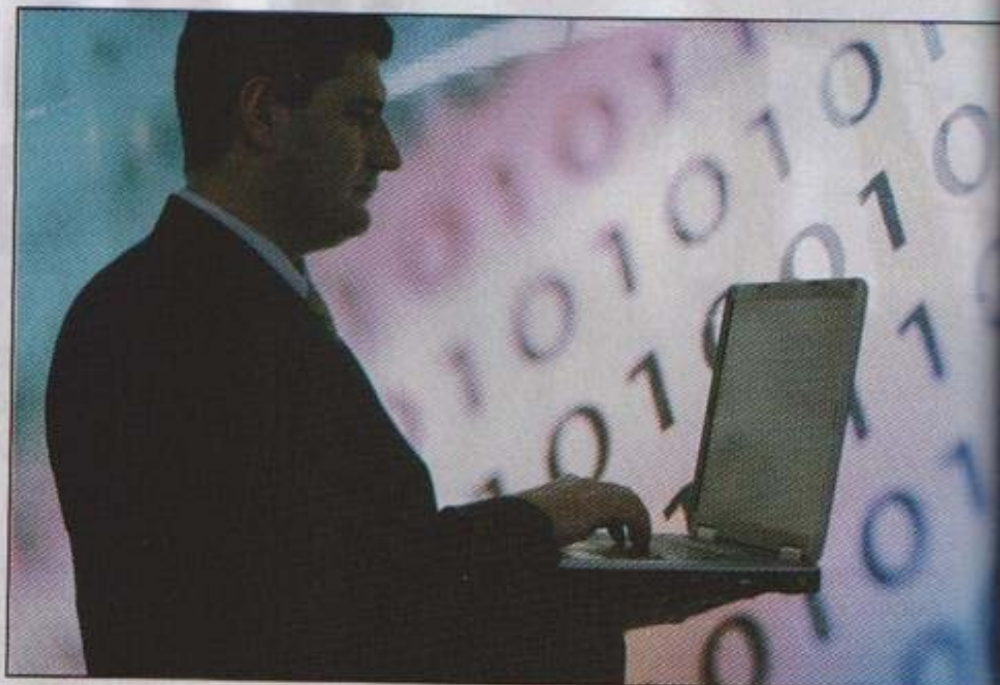
El escándalo desatado por la publicación en Internet de los correos electrónicos y passwords de periodistas, jueces y funcionarios reavivó una vieja polémica sobre la seguridad informática. Y planteó varias preguntas: ¿podría haberse evitado el hackeo? ¿Cómo se descubrió la maniobra?

"Existen formas de saber si quien manda un e-mail es quien dice ser", afirma Pablo Masoero, presidente de Bacom, una firma especializada en seguridad informática. "El cifrado y la firma digital evitan la suplantación de identidad", asegura.

En la Argentina, según una investigación de la revista *Noticias*, se espían 50 mil comunicaciones diarias (entre mails y teléfonos pinchados). No obstante "las herramientas de seguridad para impedirlo se usan poco", lamenta Masoero.

Existen en el mercado varios softwares de cifrado que se basan en la utilización de algoritmos matemáticos para transformar los datos en una forma ininteligible. "Con esta técnica se encripta la información y se eluden los riesgos de captación del contenido del mensaje y el análisis de tráfico por parte de terceros", explica Masoero.

El cifrado tiene dos variantes: los de clave simétrica usan la misma



combinación para cifrar y descifrar, y los de asimétrica emplean distintas.

El concepto de la firma digital se basa en la verificación de la autoría de un mensaje. Esto quiere decir que el destinatario puede comprobar que el supuesto remitente es quien dice ser; además de verificar la integridad del mensaje, ya que la firma digital se genera junto con el texto e impide cualquier modificación una vez que ha sido enviado.

Los mecanismos de cifrado y firma digital sirven también para evitar la interceptación de un mensaje por un tercero y la posterior retransmisión al destinatario original; o que el emisor o el receptor nieguen la transmisión del mensaje (lo que se conoce como "no repudio").

CELULARES ROBADOS. No sólo la in-

trusión en correos electrónicos ajenos (considerada una forma de violación de correspondencia), sino también otros tipos de delito pueden ser detectados, cuando no evitados, mediante el uso de la tecnología.

El robo de celulares, que según datos de la Cámara de Informática y Comunicaciones alcanza a las 300 mil unidades anuales, es uno de los flagelos que pueden ser combatidos tecnológicamente.

La firma ATS desarrolló un software que permite a los operadores de telefonía celular bloquear las llamadas provenientes de celulares robados. El sistema, denominado Equipment Identity



"El cifrado y la firma digital evitan la suplantación de identidad".

PABLO MASOERO



Se puede determinar si un celular está en una lista negra, gris o blanca, y decidir su eventual bloqueo.

Register (EIR), funciona en las redes GSM de telefonía celular (las que utilizan el "chip").

En la tecnología GSM, los equipos tienen dos sistemas de identificación. Un número corresponde a la terminal y otro al chip. "Cuando un teléfono es robado, usualmente se le cambia el chip para poder venderlo -dice Pablo Ricobelli, gerente regional de ATS-. Lo que hace el sistema es verificar si ambos códigos de identificación (el del chip y el de la carcasa) coinciden". De acuerdo a esto se determina si el teléfono está en una lista negra (denunciados por robo), gris (en observación) o blanca (aptos). Con esta información, el operador decide si bloquear, habilitar o realizar el seguimiento del teléfono móvil.

FRAUDES EN EL SISTEMA DE SALUD. Según datos de la ANMAT, entidad que controla la calidad y seguridad de alimentos y remedios, "casi el 7% de los medicamentos que circulan son ilegítimos, incluyendo los robados, adulterados, contrabandeados, los que se elaboran en farmacias sin autorización y los falsificados". Para mitigar este problema, la compañía de software Commed y la Asociación Argentina de Farmacéuticos de Hospital (AAFH) crearon el FARO, un sistema de identificación única de medicamentos, destinado a prevenir su adulteración o robo.

El FARO se basa en un sistema de identificación por radiofrecuencia (RFID), que incluye una etiqueta con un alambre de cobre que guarda datos como el número de lote y de partida, fechas de elaboración y vencimiento, código de

HERRAMIENTAS CONTRA EL CRIMEN

PROBLEMA	SOLUCIÓN
Violación de casillas de e-mail	Software de encriptación y firma digital.
Robo de celulares	EIR (Equipment Identity Register).
Falsificación y robo de medicamentos	FARO: Identificación y seguimiento de medicamentos por radiofrecuencia (RFID).
Sobrefacturación en medicina prepaga	PROFILING: detecta prácticas médicas incorrectas o innecesarias.
Lavado de dinero	Software que cruza datos de operaciones bancarias, compraventa de inmuebles, etc.
Delitos combinados	I.2: software que cruza información de varias fuentes y bases de datos.



producto, cantidad y precio. El sistema fue diseñado para preservar la identidad del paciente y las cifras de ventas de los laboratorios. Así, antes de comercializar un medicamento, el farmacéutico puede verificar su procedencia.

La sobrefacturación y los fraudes en los sistemas de salud prepagos también pueden detectarse mediante el software adecuado. El sistema de "Profiling" creado en Swiss Medical permite detectar prácticas incorrectas o innecesarias de acuerdo al tipo de especialidad. "La utilización de este sistema se traduce tanto en un ahorro de costos como en una mejora de la atención médica", dice Beatriz Armand Ugon, jefa de soporte de Información de la prepaga. El Profiling "utiliza un generador de reportes para analizar grandes volúmenes de información con un display amigable, y compararlo con promedios históricos en cada especialidad", agrega Ugon. Fue desarrolla-

do por el departamento de sistemas de Swiss Medical y consultores de Microstrategy, una firma local de software ERP. La idea es que pueda ser útil para cualquier auditor médico sin necesidad de un especialista en sistemas.

FRAUDE BANCARIO. Según un informe del BID difundido en diciembre de 2004, la Argentina encabeza el triste ranking de lavado de dinero por canales bancarios. Las normativas internacionales son cada vez más estrictas con la banca local y les exigen la adopción de sistemas de detección de lavado. Compañías globales como Sybase y Sofrecom desarrollan este tipo de software que permite cruzar enormes volúmenes de información provenientes de fuentes dispersas y detectar patrones anómalos en transacciones financieras. Estos sistemas son útiles para la investigación de delitos financieros, fraudes impositivos y en el sector de seguros. Uno de estos software, el I.2, cobró notoriedad durante la investigación del robo a las cajas de seguridad de la sucursal Acassuso del Banco Río, cuando detectó la compra de un inmueble y contactos telefónicos entre miembros de la banda.

Así como el Excalibur se hizo famoso en el caso Cabezas, porque podía cruzar millones de llamadas, "el I.2 puede incorporar bases de datos de compañías aéreas, cuentas bancarias, registros de propiedad y otros", explica Claudio Licata, gerente de Global Software, la compañía que lo comercializa en el país. Con los resultados de los cruces, el sistema traza diagramas y gráficos que representan las distintas hipótesis de investigación y busca nuevas correlaciones y pistas. Un verdadero Watson para todo Sherlock Holmes.



GABRIELA ENSINCK



APLICACIONES. *Mails, lavado de dinero, medicamentos y documentos son algunos de los campos de trabajo.*