CINCO DÍAS
24/03/2000
20.3d

PROC.: MADRID
PERIOD.: DIARIA
OJ. ÚTIL: 49.921
OJD DIF.: 28.581
TEL.: 91 538 61 00
WEB: www.gdm.es
E-MAIL: gdm@gdm.es

Las pérdidas por fallos de seguridad superan los 800.000 millones

Los delitos en la Red

La popularización de Internet y el comercio electrónico, junto al imparable desarrollo de las nuevas tecnologías, no evitan la proliferación del fraude en un entorno que cambia tan rápidamente como el avance tecnológico y la astucia de los criminales cibernéticos

LEO MARTÍN

Narcotraficantes operando en un entorno virtual, creadores de virus informáticos, terroristas, estafadores, pedófilos, defraudadores telefónicos, inversores sin escrúpulos que utilizan la Red para generar falsas noticias y afectar a su antojo las cotizaciones bursátiles, *ciberextorsionadores* o *ciberokupas* del *.com*, que se apropian rápidamente de los dominios corporativos, son ejemplos de la adaptación del delito a los nuevos tiempos.

El caso más reciente fue el de Yahoo!, eBay, Amazon o E*Trade. Conforme bajaba la cotización de estas compañías y subía la de las empresas de seguridad, inversores, usuarios y empresas se preguntaban: "Si estas compañías, nacidas de la Red, son vulnerables, ¿quién no lo es?".

La sensación al asomarse a la www es, como bien resumía recientemente un experto en derecho informático, "de indefensión". La lucha contra el ciberdelincuente –y su posterior enjuiciamiento– plantea enormes dificultades, no sólo desde el punto de vista técnico sino legal.

Los delincuentes afrontan multas y penas de prisión, que oscilan entre los seis meses y los cuatro años

"Elaborar dictámenes periciales para la obtención de pruebas –datos de conexiones telefónicas que deben dar los operadores sólo bajo petición judicial–, cuantificar los daños y perjuicios ocasionados; identificar a los autores, que suelen utilizar claves de otros usuarios; junto a la falta de preparación técnica en muchos de los profesionales de la justicia" son las razones que aduce Francisco Hernández Guerrero, fiscal del Tribunal Superior de Justicia de Andalucía, especialista en delitos informáticos.

Delitos y delincuentes

Hace unas semanas, compañías como E*Trade, Amazon, Yahoo! o eBay no pudieron satisfacer las demandas *web* de sus usuarios. Se calcula que la técnica de *denegación de acceso* que colapsó Yahoo! le costó casi medio millón de dólares –más de 80 millones de pesetas– en sólo tres horas. Sus autores fueron presuntamente unos adolescentes,conocidos como *Mafiaboy* y *Coolio*, quienes se enfrentan a fuertes penas en Estados Unidos.

En España, la cosa cambia. Los delincuentes de la Red afrontan penas de prisión que oscilan entre los seis meses y los cuatro años, o multas, siempre que los daños que causen sean superiores a las 50.000 pesetas. Unas condenas poco disuasorias. ¿En cuánto se valora la modificación de un fichero log? ¿Quién puede evaluar esto? Además, muchas veces ni empresas ni usuarios saben que han sido atacados. La mayor parte de los delitos informáticos son, de hecho, *invisibles*.

Para Jordi Murgó, experto en seguridad informática, "los ISPs y los operadores tienen cierta responsabilidad". Murgó considera que, si ya se han establecido controles para que los usuarios entren en las *web* empresariales, ¿por qué no poner controles similares para salir a Internet?".

En España, los *ciberdelitos* se clasifican en dos grandes grupos: aquellos contra la intimidad o privacidad informática y los patrimoniales. Aquí entran los delitos de fraude (estafas informáticas y uso indebido de terminales y equipos); daños a documentos o programas; espionaje empresarial y contra la propiedad intelectual (pirateo informático).

Aunque gran parte de los delitos informáticos los originan usuarios del propio sistema –empleados despedidos, por ejemplo–, los ataques que más suenan son los cometidos por delincuentes externos: "El caso de Yahoo! ha sido un asunto de *ciberextorsionadores*", asegura Murgó.

Hernández distingue entre el afán de lucro de los delincuentes, ya sean estafadores electrónicos, piratas informáticos, defaudadores de líneas, equipos telefónicos o espías empresariales, y los perseguido saboteadores (*hackers*). "Estos últimos no son considerados delincuentes en este sentido, pues entran en los sistemas sin ánimo de violar datos personales u obtener información económica, aunque pueden serlo por las informaciones que introducen en los ficheros de registro de los sistemas", asegura. Como destaca la psicóloga Sonia Navarro, "son adolescentes con una conducta similar a los de otros tiempos, sólo que se mueven en un entorno diferente, el de Internet".

Éxitos y fracasos

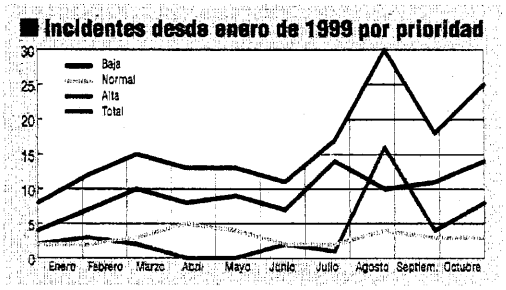
El FBI estima que las pérdidas anuales por fallos de seguridad informática superan los 5.000 millones de dólares –825.000 millones de pesetas–. Sólo en España, el mercado de seguridad y virus informáticos mueve unos 100.000 millones. Los incidentes más relevantes han sido los siguientes:

- **Febrero de 2000:** la Brigada de Delitos Tecnológicos y de la Información de la Policía detiene a Tío Willy acusándole de varios delitos de pornografía infantil a través de Internet. El detenido presuntamente publicaba imágenes pornográficas de menores en Internet, usurpaba los accesos a las cuentas de la Generalitat de Cataluña y ocultaba su identidad bajo complejos sistemas de encriptación.
- **Febrero de 2000:** unos *cibervándalos* argentinos firmaron supuestamente un mensaje reivindicativo en la portada de la *web* del Banco Popular. Querían que los dejasen en paz.
- **Enero / febrero de 2000:** a través de la operación millenium, más de cien agentes de la Guardia Civil detienen a 55 personas en España, acusadas de fraude en telecomunicaciones. Pertenecían a la denominada red COM30, dedicada a fraudes telefónicos a través de líneas 900 y a clonar tarjetas de telefonía móvil. La operación comenzó con la detención de un individuo que se dedicaba a realizar compras por Internet con una tarjeta de crédito perteneciente a otro usuario.
- **Diciembre de 1999:** la operación HENRY se convierte en la desarticulación de la primera red de estafa por Internet detectada en la UE. Los detenidos fueron acusados de fraude electrónico por Internet. Enviaban por correo

Ciberpolicías europeos

Nacidos como los delincuentes informáticos, al abrigo de las nuevas tecnologías, las fuerzas de seguridad han cambiado la placa y pistola por el PC y el módem. El Grupo de Delitos de Alta Tecnología (GEDAT) de la Guardia Civil, nacido en 1997, realiza medio centenar anual de detenciones relacionadas con delitos informáticos. Parece poco, visto el ritmo de crecimiento de los incidentes, que se duplica cada tres meses, según el centro de Coordinación de Emergencias de Redes Telemáticas (CERT), entidad encargada de orientar y coordinar a empresas, usuarios y fuerzas de seguridad del Estado.

En diciembre de 1999, la Universitat Oberta de Catalunya puso en marcha el denominado Proyecto Falcone (http://falcone.uoc.es). Entre diciembre del pasado año y febrero de 2000, un centenar de policías españoles, italianos y alemanes exploraron, mediante un campus virtual, las nuevas formas de criminalidad informática organizada, derivada de la aplicación de las nuevas tecnologías. Estos *ciberpolicías* europeos investigan los riesgos y nuevas formas de *ciberdelincuencia*, especializándose en el más reciente sector de riesgo de la sociedad electrónica: la informática e Internet.



➤ ➤ ➤