

Los riesgos de la Red

En la actualidad asistimos a un incremento cada vez mayor del acceso de los ciudadanos a los sistemas que ofrece la llamada Sociedad de la Información. Más concretamente, Internet, la red de telecomunicaciones capaz de conectar al mundo entero entre sí, es ya una realidad para millones de ciudadanos. Gracias a ella se puede hablar verdaderamente de un mundo globalizado donde las fronteras no constituyen límite alguno. Pero esta imagen tan positiva se ve ensombrecida por los casos de ciberdelincuencia que cada día salen a la luz. Porque no es oro todo lo que reluce...

Carolina López Álvarez

A MENUDO llegan noticias sobre la disminución de la brecha digital, es decir, del espacio que existe entre los ciudadanos «conectados» y los «no conectados». La brecha digital cada vez es menor, sobre todo en los países desarrollados, donde los gobiernos luchan porque su nación sea la que más hogares conectados posea, más banda ancha disponga o en la que mejor funcione aquello que se ha denominado como administración electrónica o e-administración. Son ampliamente conocidas las ventajas y beneficios que este progreso tecnológico ha traído consigo pero conviene pararse a pensar acerca de los perjuicios y aspectos negativos que todo avance lleva intrínsecamente relacionado. Se trata de analizar los riesgos que conlleva la existencia de una mega comunidad conectada donde los individuos que la habitan no pueden ser plenamente identificados, donde no existen sistemas de seguridad que protejan con plenas garantías y donde, como en todas las comunidades, existen negocios de los que algunos intentarán aprovecharse. Es en este panorama en el que aparecen y proliferan una serie de delitos que si en algunos casos ya existían en la sociedad real, ahora, a través de la Red, adquieren mucho más poder. Carlos Jiménez Suárez¹, segundo vocal de la Junta del Colegio Oficial de Ingenieros de Telecomunicación (COIT), indica en este sentido que Internet permite atacar de forma indiscriminada a un número incalculable de internautas con mayor rapidez y, en definitiva, con un impacto superior.



Pérdida de confianza

Si hay alguna característica de Internet especialmente aprovechada en estos momentos es la falta de identificación de los interlocutores. Sin embargo, este hecho también constituye precisamente un factor en contra de la evolución de las transacciones electrónicas ya que la gente no posee la confianza suficiente para realizarlas con la completa seguridad. Según Jiménez Suárez, «la poca confianza que hay en Internet es lo que hace que el comercio electrónico no progrese a los niveles que debía hacerlo».

Para Enrique Martínez Marín, director general del Instituto Nacional de Tecnologías de la Información (INTECO), los efectos negativos de las amenazas

informáticas pueden ser tanto económicos como de pérdida de confianza en el ámbito de Internet. Así lo afirma en el *Informe sobre Fraude Online 2006* que fue presentado el pasado mes de abril. En el mencionado informe, Martínez Marín hace referencia a la necesidad de coordinación de actuaciones entre las distintas instituciones, tanto públicas como privadas, tanto en el ámbito nacional como internacional, para intentar luchar contra estas acciones fraudulentas. Para ello, se debería poder compartir la mayor cantidad de información posible. Asimismo, el director del INTECO resalta la idea de «proteger la tecnología apoyándonos en la propia tecnología» como ya están haciendo las entidades bancarias u otros

1. Carlos Jiménez Suárez es también presidente de la Plataforma Tecnológica Española para la Seguridad y la Confianza (eSEC) y presidente de la empresa SECUWARE.



Foto: CE

«Internet permite atacar de forma indiscriminada a un número incalculable de internautas con mayor rapidez y, en definitiva, un impacto superior», afirma Carlos Jiménez del COIT

como los relacionados con menores, es el caso de la pornografía infantil u otros delitos sexuales.

Una de las actividades fraudulentas más comunes, continúa Pérez Subías, tiene que ver con la estafa y consiste en la obtención de datos privados a través del envío masivo de correos electrónicos que conectan al usuario a páginas Web falsas (de entidades bancarias, por ejemplo) donde se le solicita sus datos, números de la tarjeta de crédito, contraseñas, etcétera. Es lo que se conoce como *phishing*. La venta fraudulenta de productos, como cursos o medicamentos, que no son verdaderamente lo que se anuncia también es una práctica bastante extendida.

Cultura de la seguridad

Carlos Jiménez Suárez (COIT) coincide con Martínez Marín (INTECO) al señalar que es necesaria la implantación de medidas preventivas que vengán a complementar todos aquellos esfuerzos tecnológicos que se realizan en la lucha contra las amenazas informáticas.

De este modo, consideran la formación como uno de los mecanismos para evitar la propagación de estos delitos. Según Jiménez Suárez, «lo más importante es educar a los usuarios; que sepan cuáles son las reglas del juego, las

organismos, como es el caso de los colegios profesionales, a través de la implantación de sistemas de seguridad como el protocolo seguro (https), factores de autenticación, firma y certificado digital o tarjeta de coordenadas, entre otros. El desarrollo y verdadera implantación del DNI electrónico constituirá en este sentido todo un avance.

Por un beneficio económico

Desde que se empezara a hablar de Internet y nuevos conceptos se implantaran en nuestras mentes, casas y oficinas, se extendió la amenaza de posibles ataques a los ordenadores, por ejemplo, por parte de virus lanzados por *hackers* (o personas expertas en las tecnologías de la información y las telecomunicaciones) que tan solo pretendían demostrar su inteligencia y capacidad para diseñar programas informáticos, documentos o mensajes perjudiciales para las computadoras.

El teniente José Antonio Lozano, experto fundador del Grupo de Delitos Telemáticos de la Guardia Civil, explica que desde ese momento hasta nuestros días la delincuencia ha evolucionado mucho hasta el punto en que en la actualidad existen auténticas mafias que desarrollan este tipo de prácticas de manera profesionalizada. De la misma manera que el sector de las nuevas tecnologías se complica, al menos desde el punto de vista de cualquier

usuario medio, los delitos telemáticos también son cada vez más sofisticados.

El origen de la profesionalización de los delitos a través de Internet se encuentra, según confirma Miguel Pérez Subías, presidente de la Asociación de Usuarios de Internet (AUI), en el momento en que los delincuentes ven en ello una forma de hacer negocio, es decir, un beneficio económico. Con el desarrollo de la tecnología, se han abierto también cada vez más oportunidades para estos individuos y han surgido estafas en comercio electrónico, fraudes a través de tarjetas de crédito, correos electrónicos no deseados (o *spam*) y virus para banca electrónica, por citar algunos. Asimismo, se ha asistido al incremento de otros delitos

El diccionario de los e-delitos

- **Malware:** proviene de la composición de las palabras inglesas *malicious software*, es decir, programas maliciosos. Se entiende por *malware* cualquier cualquier programa, documento o mensaje que puede resultar perjudicial para un ordenador, tanto por pérdida de datos como por pérdida de productividad. Ejemplos de *malware* son los virus, los gusanos, troyanos y *backdoors*, *spyware*, *adware* y *dialers*.
- **Crimeware:** es el conjunto de amenazas de Internet cuyo objetivo es la realización de delitos que permitan conseguir un beneficio económico, directa o indirectamente. Se puede considerar *crimeware* los troyanos (especialmente los ladrones de contraseñas y bancarios), *bots*, *phishing*, *adware*, *spyware*, *spam* y *dialers*.
- **Fraude online:** se basa en una técnica denominada ingeniería social. Mediante esta técnica, basada en el engaño, el internauta es inducido a actuar de una determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado. Las técnicas más comunes son: *phishing*, loterías falsas, webs falsas de recargas, *scam*, *pharming*, compras por Internet.

Fuente: Página Web de la Campaña contra el fraude Online y la Seguridad en la Red: www.seguridadenlared.org

ventajas y los riesgos que se corren con cada conexión a Internet». En el *Informe sobre Fraude Online*, Martínez Marín va más allá y habla incluso de la creación de una cultura de seguridad adecuada como el reto más inmediato. Hoy en día se ponen en marcha cada vez más programas de formación y herramientas técnicas que permiten identificar e incluso eliminar con mayor facilidad y rapidez este tipo de prácticas. Gracias a todo ello, los niveles de concienciación de los ciudadanos aumentan, permaneciendo más alerta de todo lo susceptiblemente falso.

Ámbito difícilmente regulable

Ante las posibles causas del incremento de estos *e-delitos*, José Antonio Lozano cree que es la falta de legislación en el ámbito internacional la que favorece el anonimato y, por tanto, hace que estos delitos sean más complicados de perseguir. Este hecho, unido a la falta de concienciación de la sociedad y al rápido crecimiento de las líneas de alta velocidad, constituyen los verdaderos impulsores de estas formas de delincuencia.

Javier Cremades², presidente de la firma de abogados Cremades & Calvo-Sotelo, considera que de momento estos asuntos están en manos de cada Estado miembro ya que existe una dificultad considerable a la hora de determinar en este tipo de delitos en la esfera internacional la presunción de autoría que permita señalar al imputado, sobre todo, por la complejidad técnica que presentan. Hay países como los de Europa del Este o aquellos que están menos desarrollados en los



Foto: CE

La falta de regulación o de legislación específica para el entorno global hace que en ocasiones los autores de estos delitos gocen de impunidad

que no existe regulación alguna ni siquiera se vigilan los contenidos. No obstante, continúa Cremades, existen instrumentos legales de colaboración que pueden dar lugar a órdenes de detención internacional, extradiciones, etc. Es el caso del convenio dictado en el seno del Consejo de Europa en el que se ha intentado consolidar la definición del concepto de la ciberdelincuencia.

El teniente Lozano explica en este sentido que las autoridades locales, en su caso la Guardia Civil, colaboran con la INTERPOL³, la EUROPOL⁴, así como con la INTERPOL latinoamericana, de cuyo grupo de trabajo de delitos informáticos son vicepresidentes.

La falta de regulación o de legislación específica para el entorno global hace que en ocasiones los autores de estos delitos gocen de impunidad. «A veces los Estados no se entienden entre sí y entre tanto puede llegar a alcanzarse la impunidad, pero, como es notorio, las fronteras están empezando a experimentar mayores grietas», afirma Cremades. El abogado considera que «como ya escribiera Thomas Friedman, dado que la tierra es plana, va a ser necesario a corto plazo establecer un derecho global en muchas materias y entre ellas estará la persecución de los delitos, especialmente la de aquellos que se realizan aprovechando Internet, uno de los «aplanadores» más eficaces.»

La combinación entre la globalización y la capacidad de alcance que posee convierten a Internet en un auténtico *monstruo* que, en palabras de Pérez Subías, tan solo es un reflejo de la sociedad en que vivimos. «El potencial de la Red amplifica estas prácticas pero debe ser la propia Red (desde proveedores a usuarios) la que busque la forma de regular este ámbito para alcanzar un equilibrio de seguridad», afirma el presidente de la AUI, Miguel Pérez Subías. ■

Enlaces de interés

Colegio Oficial de Ingenieros de Telecomunicación: www.coit.es
 Observatorio del Notariado para la Sociedad de la Información: <http://www.notariado.org/observatorios/socinf/>
 Asociación de Usuarios de Internet: www.aui.es
 Grupo de Delitos Telemáticos - Guardia Civil: <https://www.gdt.guardiacivil.es/>
 Plataforma Tecnológica Española para la Seguridad y la Confianza: <http://www.aetic.es>
 Campaña contra el fraude online y la Seguridad en la Red: <http://www.seguridadenlared.org>
 Instituto Nacional de Tecnologías de la Comunicación: <http://www.inteco.es>
 INTERPOL: <http://www.interpol.int>
 EUROPOL: <http://www.europol.europa.eu/>

2. Javier Cremades, además de ser abogado en ejercicio, es miembro del Consejo Asesor para la Administración Electrónica del Ministerio de Administraciones Públicas y presidente del Observatorio del Notariado para la Sociedad de la Información.

3. Es la organización internacional de la policía. El nombre oficial es ICPO-Interpol cuyas siglas corresponden a Organisation internationale de police criminelle – Internacional Police.

4. Es la contracción de la Oficina de Policía Europea (the European Police Office).