

La internet, espacio del delito

A pesar de programas antivirus y de protección de identidad, al navegar nadie está seguro en la red.

22 de Abril de 2004

Para los cuerpos policiales y de investigación, las "andanzas" de los malvados en internet agregan no pocas variantes al crimen organizado. La pornografía infantil, las actividades de los hackers, las acciones contra la propiedad intelectual y los fraudes, son los principales campos de actuación de las autoridades.

Nadie está seguro en la red

La tecnología crea sus dioses y sus demonios. Cuando el hacker logra acceder a la clave de su profesor universitario y jugarle una mala pasada, alguno sonríe y hasta celebra el "pecado juvenil".

Pero otros cambian la risa por la indignación cuando conocen, por ejemplo, los procedimientos de quienes se valen de los recursos de internet para intercambiar las crudas imágenes de menores sometidos al drama de la pornografía infantil.

Juan Salom Clotet, comandante jefe del grupo de delitos telemáticos de la Guardia Civil de España explica que son cuatro los delitos informáticos: la pornografía infantil, los fraudes en internet, la actuación de los hackers (virus, accesos...) y los actos contra la propiedad intelectual.

Con excepción de la pornografía infantil, son delitos privados, es decir, los debe denunciar la víctima.

Salom participó en el reciente Congreso sobre "Seguridad, Defensa e Internet", organizado por el Seminario de Estudios de Defensa de la Universidad de Santiago de Compostela y el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), en la ciudad de Santiago de Compostela, capital de Galicia (norte de España).

Las unidades de delitos telemáticos realizan una actividad cotidiana de supervisión de la red, pero es la denuncia la base de cualquier actuación.

¿Cómo opera una unidad de este tipo?

Si un ciudadano expone la pérdida de 10 mil euros (alrededor de 12,800 dólares) de su cuenta por una transacción en banca electrónica, los especialistas (el principal capital de la unidad), revisan el equipo del afectado y, en el caso del banco, con una orden judicial, inspeccionan en la búsqueda del equivalente a la huella tradicional.

El investigador se apoya en las exigencias de la nueva tecnología sin obviar las prácticas clásicas.

"Con mi investigación tecnológica voy a llegar al computador pero no sé quién está detrás. Lo puedo conseguir en una casa (con un único usuario); en una empresa (de unos mil trabajadores) o en un ciber, donde impera el anonimato", afirma el investigador.

Es complejo y a veces, al llegar "al mundo real", muere la investigación por la imposibilidad de localizar al delincuente.

Una alarma social

En el caso de la pornografía infantil, Salom Clotet observa un salto del estereotipo clásico del pederasta (persona adulta, que vive solo y es tímido o acomplejado por sus inclinaciones sexuales), hacia personas "más jóvenes y osadas".

Cita a los estudiosos del tema, quienes observan en "el consumo abusivo de pornografía desde tempranas edades" la explicación del fenómeno.

"La persona inmadura, al llegar al hastío, busca cosas más raras; desviaciones. Poco a poco llega a los bebés. Son imágenes que causan verdadera conmoción", señaló.

Por otra parte, "como en internet todo se cuenta, con los foros refuerza su comportamiento", al ver que no es el "único bicho raro". De la observación pasa a la pederastia, al turismo sexual. Y de ahí a organizar su propia galería de imágenes. Filma y fotografía sus actos sexuales.

Ocurre que en los últimos tiempos los organismos de investigación han detectado la intensa cotización en internet de las colecciones de los pederastas.

Curiosamente quienes participan en estas prácticas no buscan dinero, sí caché y prestigio. Es intercambio de morbo. La unidad central de la Guardia Civil inspecciona todas las páginas de este tipo alojadas en España. Si están en el extranjero, informa a los cuerpos de seguridad.

Hay auténticos "paraísos informáticos" en los cuales los pederastas actúan con impunidad.

Todos los casos responden al mismo patrón: quien consume pornografía infantil, luego la practica.

El investigador puede llegar al delincuente por una fotografía "colgada" en la red y descubrir, al investigar la computadora y el sitio de los hechos, más imágenes, incluso con familiares, adolescentes y bebés, además de vídeos en directo.

Hacker: el más complejo

A Salom Clotet le cuesta decirlo, pero lo dice: "Internet, hoy en día, es un espacio de impunidad".

Observa que "si bajo la defensa del anonimato eliminamos las medidas de control en internet y hacemos impune el delito, será la muerte de la red".

El delito informático, razonó, existe y crece.

Esta agresión no viene por vía de la "amenaza fantasma de empresas comerciales y gobiernos", sí por la actuación de "quienes vulneran nuestros derechos", como es el caso del hacker, experto conocedor de los sistemas informáticos y con capacidad para robar desde una clave de acceso a la banca hasta causar un problema de Estado.

Esta astucia criminal es el obstáculo a vencer. "Estamos creando una paranoia con la defensa de la intimidad en internet frente a enemigos que no son tales enemigos (empresas y gobiernos)", observa Salom, quien destaca la existencia de instrumentos jurídicos como la Ley de Protección de Datos (en el caso español), una de las más exigentes del mundo, defensa del usuario en el ámbito jurídico.

Fraudes en la red

En los casos de propiedad intelectual, las unidades de delitos telemáticos lo tienen difícil, en particular porque es difícil determinar los límites de la propiedad en acciones intangibles como descargar música sin pagarla.

Con respecto a los fraudes en la red, funciona el clásico timo y el fraude. Los timos, destaca el experto, han existido toda la vida en el mundo real y se exportan al mundo virtual.

Explotan la ingenuidad del usuario de mil formas: desde proponerle "partir" la herencia de un dictador africano recién fallecido (previo pago del IVA), hasta anunciarle que es el ganador de la lotería, si bien en su vida ha jugado.

Con respecto a la banca electrónica la considera muy segura. El problema comienza cuando la gente no custodia bien su clave.

Del lado del comercio electrónico hay una curiosidad: contra toda idea, el 70 por ciento de los fraudes son del cliente hacia el comerciante. Ocurre, por ejemplo, cuando se compra un libro y el número de la tarjeta de crédito es falso.

El trípode de la seguridad

"El 95 por ciento de los delitos se reducirían si nuestras computadoras fueran seguras", sostiene.

Esta seguridad está integrada por un "trípode invencible": antivirus, sistemas operativos actualizados y un buen cortafuegos, "gratuitos en la red y muy eficaces".

Xosé Antonio Vila Sobrino, profesor titular de Ciencias de la Computación de la Universidad de Santiago de Compostela y en su ponencia, "Técnicas de protección de la privacidad en el mundo digital", le recordó al desprevenido usuario algunos "alertas" que no debe ignorar:

Al visitar una página web la persona se puede registrar de manera involuntaria en algún sitio. Cuando ocurre ese registro aumenta la posibilidad de recibir "ofertas especiales", no deseadas. La web fue diseñada para transmitir información, no para protegerla. El usuario cuenta con medidas legales para proteger su intimidad (Ley de Protección de Datos) pero también debe poner en práctica normas de auto-regulación como elegir un buen proveedor de acceso a internet (con políticas de seguridad) o disponer de claves de acceso fuertes y blindadas (puede ser una clave base con variantes).

Los conflictos sobre seguridad no se limitan al ámbito de lo privado. El Estado asume sus propios "dolores de cabeza" en este terreno.

Néstor Ganuza Artilles, ejecutor del Plan Director de Sistemas de Información y Telecomunicaciones del Ministerio de Defensa de España y en su intervención "Seguridad de la información en Defensa", insistió en un aspecto vital para las grandes corporaciones: la ingeniería social.

Es decir, de nada valen los cortafuegos, los antivirus o las máximas precauciones con los sistemas informáticos, si luego no se destruyen las fotocopias o no se supervisan las reuniones con la gente.

"Proteger un sistema es difícil, pero colocar un micrófono en una sala de reuniones es sencillo". A partir de esta máxima sigue otra: "El enemigo siempre ataca lo más vulnerable".

Las medidas de protección no deben olvidar a nadie: personas, instalaciones, documentos y empresas merecen igual atención a la de un ordenador de cuya aparente inocencia ya nadie se puede fiar.

El reto jurídico de la web

José Julio Fernández Rodríguez, profesor titular de Derecho Constitucional de la Universidad de Santiago de Compostela y codirector del Seminario de Estudios de Defensa de la USC-

CESEDEN, reconoce que "los avances tecnológicos ejemplificados en la red, han provocado unos cambios de índole cuantitativa y cualitativa en la vida de la persona y en el funcionamiento social que exigen una rápida adaptación del ordenamiento jurídico".

"No obstante, este proceso de aclimatación del Derecho a la nueva realidad -añade- no debe perder los logros que para los derechos fundamentales y las libertades públicas atesora el Estado democrático".

El especialista es autor del texto "Secreto e intervención de comunicaciones en Internet", próximo a publicarse en Madrid.

En las conclusiones expone que "el derecho al secreto de las comunicaciones requiere especial atención en la actualidad", por cuanto "el progreso tecnológico lo ha sometido a nuevos peligros. Su vulneración afecta tanto a la libertad como a la intimidad, además de provocar en la ciudadanía un sentimiento de inseguridad".

"El origen liberal del derecho y, por lo tanto, su perfil de derecho de defensa, es compatible con una concepción activa del mismo que trate de otorgarle una protección horizontal, es decir, frente a particulares y no sólo frente al Estado. Los avances técnicos, ejemplificados en Internet, obligan a una reformulación del derecho que complete las reducidas dimensiones que aquel origen liberal le otorgaba".

Propone actuar con precisión "a la hora de delimitar las categorías jurídicas implicadas y ganar, así, dosis de certeza y seguridad frente a los riesgos de promocionar la flexibilidad del aplicador".

El jurista observa dos modos de comunicación en internet: por canal cerrado (entran en el ámbito de cobertura del derecho), como el correo electrónico, la telefonía, la videoconferencia, el envío de mensajes SMS y "el chat en la opción cerrada a dos usuarios".

Las abiertas (no protegidas por este derecho), como los grupos de discusión, la televisión, la radio o los chat cuando no son de dos.

La justificación de la injerencia, observa, debe realizarse con especial rigor. "Está claro que la regla general es la vigencia del derecho al secreto de las comunicaciones y la excepción su intervención. La concesión de la autorización judicial para la intervención debe darse de manera restrictiva".

La legislación actual, afirma, "muestra claras insuficiencias y falta de adaptación a la realidad digital de la Sociedad de la Información. La solución ante este panorama pasa por realizar las oportunas reformas legislativas", y entender que "internet es un nuevo medio y una nueva forma de comunicación", no asimilable a los sistemas anteriores.

En las conclusiones expone que "el derecho al secreto de las comunicaciones requiere especial atención en la actualidad", por cuanto "el progreso tecnológico lo ha sometido a nuevos peligros. Su vulneración afecta tanto a la libertad como a la intimidad, además de provocar en la ciudadanía un sentimiento de inseguridad".

Fuente: noticiosas.