Los casos más usuales de criminalidad informática y cibernética

DANIEL R. NIELSEN*

Agente supervisor especial del FBI (Oficina Federal de Investigación)
de los Estados Unidos de América

1. LOS DELITOS RELACIONADOS CON LOS ORDENADORES

Actualmente —y esto lo sabemos todos—, nos encontramos en el paso de la era industrial a la era de la información. En el rol tradicional de la policía uno de los objetivos de su actuación consiste en la preservación de los bienes y los derechos entendidos o vinculados a elementos materiales. Con el cambio de era, estos bienes materiales evolucionan hacia un concepto lógico, menos tangible físicamente, pero con el mismo grado de relevancia por lo que se refiere a la necesidad de protección legal y actuación policial. Por este motivo, las ideas y los servicios adquieren mucha más importancia al lado de las cosas materiales en el sentido tradicional. Pero, como policía, hay que proteger las ideas y los pensamientos de la misma manera que se protegen los bienes materiales.

Por esto, si tenemos suficientes recursos y conocimientos para valorar el impacto de las nuevas tecnologías en la comisión de los delitos, podremos integrarlas también en la investigación y facilitar su adaptación a los nuevos retos que se nos presentan.

Con todo, aparte de los conocimientos y de la experiencia profesional de cada uno, de cada policía, es muy importante que todos los cuerpos de policía del mundo trabajen en común para hacer frente a la criminalidad informática y cibernética. La comisión de los delitos relacionados con los ordenadores suele tener un carácter transfronterizo, por ello les quiero transmitir esta idea, que, para

---

* Anteriormente, Nielsen había trabajado siete años como oficial de la policía de Seatle. Ahora hace doce años que trabaja en el FBI. Al principio era miembro de las unidades especializadas en la lucha contra los grupos organizados; más adelante trabajó en el análisis forense de los ordenadores. Actualmente, es agente supervisor especial de las brigadas de investigación de los delitos cometidos contra los ordenadores que se encuentran en el área geográfica del noreste de los Estados Unidos.

mí, es fundamental, es decir, que la colaboración internacional en este ámbito es imprescindible para llevar a cabo las investigaciones.

Ante este tipo de delitos, primero hay que tener en cuenta una doble perspectiva: por un lado, los ordenadores y las redes informáticas pueden ser el *medio* utilizado para cometer los delitos y, por otro lado, pueden ser el *objeto* del hecho ilícito.

Respecto a los sistemas informáticos, debemos considerar sus puntos vulnerables, que se pueden clasificar en cuatro categorías:

a) los puntos vulnerables del propio ordenador, como por ejemplo la utilización de contraseñas poco sólidas;
b) los basados en la red, como por ejemplo los puntos de entrada desprotegidos;
c) los basados en el lugar de instalación del sistema, como el caso de los servidores situados en zonas abiertas, o el acceso franco a personas que no son lo bastante conocidas;
d) los basados en las personas: por ejemplo, en los casos de personal con contratos temporales y casos de despidos, supone un gran riesgo comunicar a una persona que administra un sistema que al cabo de treinta días se le despedirá.

Estos puntos débiles de los sistemas ante lo que significa la nueva era de la información comportan también amenazas nuevas con sus peculiaridades, que podríamos resumir en los puntos siguientes:

a) una gran facilidad para obtener los instrumentos necesarios para producir el daño (por ejemplo, los *hackers*[1] pueden obtenerlos por vía Internet);
b) estos instrumentos están muy distribuidos y se pueden utilizar sin necesidad de tener muchos conocimientos ni demasiada preparación técnica;
c) la globalización de las infraestructuras implica una mayor exposición a un ataque potencial;
d) la interdependencia entre los sistemas hace que las consecuencias de un ataque sean menos previsibles y más severas.

Por todo ello, se puede decir que la estructura de telecomunicaciones es la principal víctima de esta nueva era de la información.

En relación con la procedencia de las amenazas, hay que decir que las más peligrosas son las que proceden del interior de una organización. Frecuentemente es mucho más perjudicial el daño que puede causar una persona que lleva el control del sistema que el daño procedente de un ataque exterior.

1. Inicialmente, la palabra *hacker* servía para definir a una persona con grandes conocimientos técnicos en informática, un experto tanto en lenguaje informáticó como en programación, que pasa muchas horas ante el ordenador para intentar encontrar los puntos débiles de los sistemas. Actualmente, este término tiene un sentido negativo porque se utiliza para definir a las personas que se aprovechan de sus conocimientos para conseguir un acceso no autorizado o dañar o destruir los sistemas informáticos y las bases de datos.

2. Los *hackers*

La figura del *hacker* se puede definir mediante una serie de rasgos característicos:

— suelen ser personas jóvenes, mayoritariamente de sexo masculino
— tienen muy pocas relaciones sociales y están obsesionados por la tecnología
— el ordenador es el sustituto de las relaciones interpersonales
— acostumbran a tener una actitud antisistémica y ansían obtener conocimientos prohibidos, impulsados por una curiosidad insaciable

El *hacker* malicioso centra sus objetivos en ordenadores, redes y sistemas telefónicos y pretende traficar con códigos de teléfono, programas informáticos pirateados, tarjetas de crédito y dispositivos de fraude en sistemas de pago.

2.1 Los métodos utilizados

Para entrar en los sistemas informáticos, los *hackers* recurren a varios métodos, como por ejemplo los siguientes:

— Intentan utilizar los *códigos por defecto*, que son los que todo el mundo conoce y entiende porque son los que aplican los fabricantes de origen.
— También pueden penetrar en los sistemas mediante los *puertos de mantenimiento*, utilizados por las grandes compañías para gestionar sus sistemas a distancia sin que se tengan que desplazar sus técnicos.
— Otro método, muy prosaico pero muy efectivo, es el llamado *dumpster diving*,[2] que consiste en remover los listados y los manuales de empresas que los han dejado por obsoletos, pero que pueden ser útiles para aplicar aquellos conocimientos a otros sistemas.
— En último término, pero no por ello menos importante, hay toda una serie de medios que llamamos *ataques técnicos*, que pueden consistir en utilizar las *puertas posteriores*,[3] con que simulan ser ordenadores con acceso autorizado, o bien en utilizar *sniffers*[4] para obtener contraseñas.

Aparte de los métodos técnicos, los *hackers* tienen otro recurso que se conoce con el nombre de *ingeniería social* y que se basa en su habilidad personal para

---

2. Traducido literalmente, significa zambullirse en los desperdicios.
3. Las puertas posteriores (del inglés *back doors o trap doors*) son un mecanismo secreto del software y del hardware que puede hacer saltar los sistemas de protección y, así, evitarlos. Se activa de una forma aparentemente inocente, porque los programadores a menudo instalan puertas posteriores en sus códigos para conectarse con el sistema y llevar a cabo algunas funciones.
4. Traducido literalmente, quiere decir husmeadores. En realidad son unos pequeños programas que buscan una cadena numérica o de carácteres en los paquetes informáticos cuando atraviesan un nodo con la finalidad de conseguir información. Normalmente, su uso es ilegal.

hacerse pasar por expertos de las organizaciones utilizando el lenguaje técnico y especializado característico de aquel colectivo, y llegan a hacer creer al interlocutor que realmente son personas de confianza.

2.2 La respuesta a la amenaza

Hay que destacar que el éxito de los *hackers* es el hecho de *compartir la información*. Por esta razón, la clave del éxito policial en la lucha contra este tipo de delitos consiste también, como premisa básica, en compartir la información con la misma facilidad.

Aunque hemos hablado de *hackers* que actúan por interés propio y de forma individual, hay que tener en cuenta la posibilidad de que actúen por encargo de gobiernos que quieran atacar las infraestructuras de nuestro Estado.

En el caso de los ataques hechos por los *hackers*, la curva de coste/beneficio o esfuerzo/resultado tradicional pierde su sentido, ya que con muy poco esfuerzo y con un coste muy bajo pueden llegar a causar daños considerables.

Entre las amenazas más frecuentes, hay que tener en cuenta estas cuatro:

— el uso malicioso de la información
— el bloqueo de los servicios
— la publicación de información reservada
— el cambio o la alteración de la información

Al mismo tiempo, se debe tener en cuenta que las amenazas pueden tener varios grados de intensidad: pueden pasar de ser simples problemas o incidencias de poca transcendencia a convertirse en delitos. En el grado más elevado, incluso pueden constituir serios problemas de espionaje o de terrorismo, con la posibilidad de desencadenar un verdadero estado de guerra (naturalmente, electrónica, en el terreno que nos ocupa). Pero, en el caso de un hipotético estado de guerra electrónica, no se identifica al enemigo de forma visible como en la guerra convencional, donde se viste un uniforme característico.

Ahora bien, para cada grado de amenaza hay diferentes organismos que se hacen cargo de ello. De acuerdo con la escala de los ejemplos del párrafo anterior, correspondería resolverlos a la policía, a los servicios de contraespionaje y al ejército, respectivamente.

Sin embargo, en un ejercicio realizado en los Estados Unidos diseñado por el ejército, donde el FBI tenía un papel de apoyo, se vio que en la práctica era el cuerpo policial el que realmente representaba la primera línea de defensa ante un ataque electrónico, mientras que el ejército tenía un papel subsidiario.

Por otro lado, actualmente una de las mayores dificultades para la investigación y la persecución de los delitos es la utilización de la criptografía en las comunicaciones a través del ordenador. No obstante, es un paso más en la utilización de la tecnología, como ya pasó primero con la aparición del teléfono y, más tarde, con la telefonía móvil. Pero es cierto que la criptografía representa un gran obstáculo a la hora de descifrar los mensajes interceptados, más aún con-

siderando que existen instrumentos de *encriptación*[5] gratuitos y bastante robustos.

3. Conclusión

Después de tratar los aspectos más controvertidos de la criminalidad informática y cibernética, quiero acabar mi exposición animando a los miembros de los diferentes cuerpos policiales a utilizar Internet —si es que no lo hacen ya— de forma particular e individual, porque podrán comprender mucho mejor el potencial y las dimensiones reales que ofrece. Es importante, por ello, perder el miedo a la tecnología.

Al mismo tiempo, les animo a conocer más de cerca y a profundizar en los delitos relacionados con la tecnología; de hecho, se trata de tener en cuenta ciertas variaciones y unos matices tecnológicos específicos e incorporarlos, a su vez, a la investigación tradicional.

5. Transformación de un texto original en uno cifrado o convencional, incomprensible para una persona que no posee la cifra o la clave.