Javier López, socio de ECIJA

Hackers ¿Héroes o villanos?

Javier López 12 abril, 2016

Son frecuentes en los informativos las noticias sobre ataques realizados por hackers a los

Esto explicaría los ataques sufridos por diferentes instituciones de la **Unión Europea** e importantes naciones, en especial Estados Unidos (Casa Blanca, NASA, etc.) e, incluso, por el mismísimo **Vaticano**. En España fue sonado el ataque sufrido en 2010 por la página web oficial de la presidencia española de la Unión Europea **(www.eu2010.es**), en la que se colgó una imagen del popular humorista Mr. Bean.

El sector privado no está exento de estas amenazas, y hace tiempo que está en el punto de mira de los ciberdelincuentes, cuyo objetivo es

apropiarse de dinero, datos, información, secretos corporativos e industriales, propiedad intelectual, etc. de las compañías, mediante la interceptación de correos electrónicos y telecomunicaciones, inutilización de sistemas de guardia criptográfica, implantación de virus, daños informáticos, phising, pharming, spam y un sinfín de técnicas cada vez más depuradas.

Sin embargo, **no todos los hackers se dedican a cometer delitos**. Y es que debido a que los servicios de seguridad de las empresas (en especial, bancos, compañías de seguros y multinacionales) muchas veces se ven impotentes ante ataques de esta naturaleza, se contrata a hackers "buenos" para tratar de paliar los efectos de estos ciberataques para que hagan el llamado "hacking ético", de forma similar a como se hacía en el salvaje oeste, donde se contrataba a antiguos pistoleros para reconvertirlos en sheriffs.

Las administraciones públicas están empezando a ver las ventajas de este sistema y, en esta línea, con la finalidad de poner a prueba su **seguridad cibernética** e identificar posibles brechas de seguridad en sus plataformas tecnológicas, el Gobierno estadounidense ha convocado una suerte de concurso llamado "**Hack the Pentagon**" en el que ofrece un sustancioso **premio de hasta 150.000 dólares si se consigue hackear la página web del Pentágono en el período comprendido entre el 18 de abril y el 12 de mayo de 2016**. Eso sí, el certamen no está abierto a todo el mundo, ya que los participantes deben ser ciudadanos de Estados Unidos, tener un número de seguridad social y registrarse en una página web del Pentágono, así como no estar incluidos en listas de terroristas, traficantes de drogas u otros crímenes.

Además, se ha establecido que los sistemas críticos dedicados a misiones concretas no se podrán hackear, de lo que parece deducirse que les consideran capaces de conseguirlo, por lo que es probable que estén más interesados en captar talento para su causa que en hacer un chequeo de su seguridad que a priori asumen franqueable.

Estos servicios de seguridad que se prestan desde el lado de la Ley, en esencia, pueden ser de dos tipos: monitorizacion, que es un producto que incluye la de vigilancia de sistemas y páginas web, en principio pasiva, sin perjuicio de que se suele acompañar de paquetes de medidas de defensa; y el citado "**hacking ético**", actividad proactiva que trata de adelantarse a la vulnerabilidad mediante la realización de múltiples pruebas para burlar la seguridad de la red para robar información sensible de la organización ("pen tests" o "penetration tests") para encontrar vulnerabilidades, sin generar daños, de forma que puedan diseñarse medidas de protección y mejorar su seguridad.

Estas ciberpruebas se instrumentalizan a través de auditorías que pueden realizarse en coordinación con los responsables informáticos de la organización, de forma que éstos sean conscientes en todo momento del grado de intrusión que están sufriendo sus sistemas, hasta el punto de que indican a los auditores (hackers) las posibles debilidades para que sean chequeadas por éstos.

Dado que este tipo de ciberauditorías no permite conocer el grado de visibilidad exterior que

Firmas


Hackers ¿Héroes o villanos?
Javier López


La democracia se fortalece con democracia
Juan Gonzalo Ospina


Sonría, por favor
Fernando Pinto Palacios


¿Qué es la realidad virtual?
Javier Puyol


¿Tiene derecho el cónyuge viudo a la vivienda ganancial que fue su domicilio?
Victoria López Barrio

pudiera existir de las vulnerabilidades, en ocasiones se solicita una **auditoría "de caja negra"**, que consiste en realizar simulaciones de ataques informáticos desde el exterior de la entidad, sin contar con ninguna información previa respecto a su infraestructura tecnológica, precisamente, para conocer las posibles visiones (pero no todas) de un eventual atacante. El test que ha convocado el Pentagono sería de esta modalidad, ya que, obviamente, no van a informar previamente sobre la existencia y localización de sus agujeros de seguridad.

Sin perjuicio de la gran utilidad de este tipo de auditorías para la **prevención de ciberataques**, no deben considerarse que las mismas sean el bálsamo de Fierabrás, pues es posible que no sean detectadas la totalidad de las vulnerabilidades, ya que se trata de una auditoría, por lo que, por definición, se hace por sistema de muestreo; y que, por su propia naturaleza, no puede ser infalible, ya que sería ciertamente improbable realizar un ataque total de todos los elementos que componen los sistemas de la organización.

Desde el punto de vista jurídico, la cuestión que puede plantearse es si en el desarrollo de estas auditorías podrían cometerse **delitos de daños a sistemas informáticos** (regulados en los artículos 264 a 264 quater del Código Penal), ya que no es extraño que los **hackers** que realizan estos ataques "pactados" alcancen el objetivo y logren acceder a los sistemas de la organización, por ejemplo, "rompiendo" contraseñas que no se les ha proporcionado previamente y recabando datos e información como prueba de haberlo conseguido.

La respuesta debe ser negativa, toda vez que la existencia de delito quedaría excluida al mediar consentimiento de la entidad que ha contratado la auditoría, pues el **Código Penal** exige que el ataque se realice "sin autorización", como uno de los elementos constitutivos del tipo penal. Es más, tal y como está configurado el servicio (detección de vulnerabilidades de forma preventiva para la mejora de la seguridad de la organización), ni siquiera podría considerarse una amenaza, pues la empresa auditora (y sus hackers) únicamente estaría honrando la obligación pactada, que tiene fuerza de ley entre las partes contratantes y deben cumplirse al tenor de los mismos (**artículo 1091 del Código Civil**).

ciberdelincuentes | ciberguerra | Código Penal | ECIJA | hackers | hacking ético

JAVIER LÓPEZ

Socio de ECIJA

Lo más leído

DESCUBRE MÁS