Hackers: un paso en falso

Hackers: Make a False Move

J.L. Rivas, V. Salgado, G. Sotelo y P. Fernández

Resumen

La Universidad de Vigo, ante el aumento de intrusiones en sus equipos (por Hackers dedicados al WAREZ), se ha decidido a colaborar con la recién creada división frente a delitos informáticos (de la Guardia Civil en Pontevedra) para evitar este tipo de ataques en un futuro. En este artículo:

- Se describirá el ataque sufrido en nuestros equipos, haciendo hincapié en las vulnerabilidades que han sido explotadas.
- Se expondrán las diferentes formas existentes para poder conta ctar con el grupo de delitos informáticos de la Guardia Civil.
- Se explicará la base jurídica de la infracción y cómo obtener pruebas incriminatorias sin violar los derechos de los usuarios e infractores.
- Se detallará cómo realizar un informe del incidente, de forma útil para ambas organizaciones.
- y se describirán los pasos que sigue la guardia civil una vez reciben la denuncia.

Palabras clave: Sistemas, hackeo, penalización, Guardia Civil, delito informático

Summary

The University of Vigo, in the face of intrusion increase (by Warez´s Hackers), has decided to collaborate with the new "Telematic Crime Group" (Civil Guard of Pontevedra) to avoid this kind of attack on the future. The content of this article:

- Describes the attack we had, making emphasis in the vulnerabil ities that have been exploited.
- Shows the different ways to contact the group of the Civil Gua rd known as "Telematic Group".
- Moreover, explains the legal base and how to obtain incriminat ory probes without transgressing users and hackers rights.
- Details how to write an incident report in a useful way for bo th organizations.
- Describes step by step how the Civil Guard works once denuncia tion has been taken.

Keywords: Systems, hacking, penalty, Civil Guard, Collaboration, Telematic Crime.

Hay infinidad de maneras de atacar y la mayoría de esta información está en Internet; sólo hay que saber buscarla y tener unos mínimos conocimientos para utilizarla

1.- Descripción del ataque

Hay infinidad de maneras de atacar y/o entrar en un sistema, la mayoría de esta información está en Internet y sólo hay que saber buscarla, por lo que cualquiera con unos mínimos conocimientos podrían utilizarla. En el caso que nos ocupa una vez que descubrieron que dicho sistema era un Windows 2000 con Service Pack 3 y que -entre otros– tenían los puertos 137 y 139 abiertos, entraron en el sistema. Una vez que se hicieron con los privilegios de administrador, instalaron el servidor FTP, *ioftpd*, para intercambiar películas, juegos, música, etc. y un robot de conexión a un canal IRC, winDrop, controlando así el servidor FTP de forma más sencilla.

2.- Contactar con la Guardia Civil

Desde 1997 existe dentro de la Guardia Civil un Grupo especializado en estos tipos delictivos, el cual depende de la Unidad Central Operativa de Policía Judicial. Con sede en Madrid abarca todo el territorio nacional y los datos de contacto son los siguientes:

URL.: http://www.guardiacivil.org/00telematicos/index.htm
Existen varios tipos de formulario, dependiendo de los hechos ante los que nos encontremos.
Teléfono (centralita) : 0034 91 514 64 00
Dirección Postal: C/ Guzmán el Bueno 110, 28003 MADRID-ESPAÑA

Debido al incremento de estos ilícitos, así como a la demanda social en todo lo relacionado con las nuevas tecnologías existen en el resto de las provincias Guardias Civiles encargados de la investigación y/o canalización a otras Unidades de estos hechos.

Para ponerse en contacto con estos Guardias Civiles integrados en las respectivas Unidades Orgánicas de Policía Judicial, basta con llamar al número de Urgencias (062), donde se nos facilitará la información necesaria para su contacto.

3.- Base jurídica de la infracción

3.1.- El delito informático

No hallamos una definición de los delitos informáticos en la legislación aunque algunos autores han ido delimitándolos

El artículo 10 de nuestro vigente Código Penal dice que "son de litos o faltas las acciones y omisiones dolosas penadas por la Ley".

Respecto a los delitos informáticos, no hallamos una definición de los mismos en la legislación. Sin embargo, algunos autores han apuntado algunas cosas como es el caso del Profesor Pérez Luño que los delimita como aquel "conjunto de conductas criminales que s e realizan a través del ordenador electrónico, o que afectan al funcionamiento de los sistemas informáticos".

Otra definición es aportada por el Profesor Davara Rodríguez, quien afirma que se trata de "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software".

A pesar de ser contemplado por la doctrina legal, no existe formalmente el delito informático como tal en nuestra legislación, ni siquiera como categoría genérica. ¿A qué llamamos pues delitos informáticos? Pues a un conjunto de delitos dispares recogidos en el Código Penal en diversas secciones los cuales tienen en común la intervención de la tecnología informática, bien como medio de comisión de la acción típica o bien como objeto del ilícito.

En general, podemos señalar las siguientes características propias de estos tipos delictivos:

1.- Rapidez en su comisión y acercamiento en tiempo y espacio.

   Un delito cometido a través de las nuevas tecnologías puede ser cometido con gran celeridad pudiendo llevar, incluso, décimas de segundo, en el caso, por ejemplo, de la activación de virus informáticos o en el robo de información mediante robots inteligentes.

   Así mismo, el espacio queda relativizado al poder ser cometidos a miles de kilómetros mediante el uso de redes de telecomunicaciones como Internet.

2.- Especialización técnica de los autores.

   La complejidad propia de las nuevas tecnologías implica un alto nivel de conocimientos, respecto a su manejo y estructura, que han de tener los autores, en términos generales, para que puedan cometer los delitos tipificados.

3.- Facilidad para encubrir el hecho y borrar las pruebas.

Debido a la naturaleza de la tecnología digital, es relativamente fácil, para un sujeto experimentado, borrar o destruir las huellas o alteraciones que haya podido causar en un sistema informático, eliminando así las pruebas que le incriminen.

Debido a las características descritas de estos delitos, se plantean los siguientes problemas que dificultan su perseguibilidad en la práctica:

1.- Determinación del sujeto

En ocasiones se puede determinar el ordenador concreto desde el que se ha cometido un hecho delictivo pero, el hecho de que una pluralidad de personas tengan acceso al mismo hace difícil la determinación del autor material del ilícito, debiendo acudir a sistemas de prueba tradicionales para esta finalidad: testigos, registros de entrada en el local, etc. que no siempre son posibles.

En ocasiones se puede determinar el ordenador concreto desde donde se ha cometido un hecho delictivo pero el que una pluralidad de personas tengan acceso al mismo hace difícil la determinación del autor material del ilícito

2.- Facilidad para ocultar pruebas o indicios

Tal y como comentábamos anteriormente, la facilidad de destruir los registros informáticos u otros indicios digitales de un delito informático por una persona con los conocimientos necesarios puede dificultar enormemente la prueba de dicho hecho.

3.- Complejidad técnica

En la línea de lo ya apuntado, estos tipos delictivos solamente pueden ser cometidos por expertos en informática y telecomunicaciones, por ello es necesario un alto grado de preparación por parte de las autoridades que persigan y conozcan de estos hechos o de sus colaboradores.

4.- Conexión de causalidad

Dado que hay un distanciamiento en el espacio e incluso en el tiempo entre el acto delictivo y el resultado pernicioso, es necesario probar la relación de causalidad entre ambos sucesos. Se debe conectar el hecho producido por el actor con el perjuicio producido, en algunos casos, a miles de kilómetros de allí.

5.- Lugar de comisión del delito

Otro problema muy común en el caso de Internet es, como ya se ha visto, la determinación del lugar donde se entiende producido el delito y, con ello, la legislación y la jurisdicción competentes para conocer del mismo. Como, por ejemplo, en la entrada de un hacker en un servidor de correo situado en los Estados Unidos cuando éste se haya conectado desde España.

Podemos clasificar los delitos informáticos en dos tipos: por un lado, los delitos clásicos que ahora pueden ser cometidos también a través de las nuevas tecnologías, y por otro lado, los nuevos delitos surgidos específicamente con ocasión de la informática y de la telemática.

3.2.- Penalización

Como hemos visto, nuestro Código Penal no contempla los delitos informáticos como tal. Por tanto, no existe un delito tipificado para la actividad del "hacking" o la intrusión en equipos y sistemas informáticos sino que tenemos varias figuras delictivas que, en función de las actividades realizadas y de los archivos accedidos por el hacker, pueden ser imputables en un caso concreto. A continuación, destacaré las que, a mi juicio, son las más importantes:

3.2.1.- Descubrimiento y revelación de secretos de carácter personal (art. 197):

El primer delito lo encontramos en el Título X del Código Penal, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, Capítulo Primero, Del descubrimiento y revelación de secretos, artículo 197 y siguientes.

1.- El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de **prisión de uno a cuatro años y multa de doce a veinticuatro meses**.

2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

El primer delito lo encontramos en el Título X del Código Penal, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio

3.- Se impondrá la pena de **prisión de dos a cinco años** si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4.- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5.- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6.- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de **prisión de cuatro a siete años**.

A los efectos de nuestro estudio, es interesante la relación de documentos objeto del tipo delictivo que realiza el artículo 197, en su párrafo 1º: "papeles, cartas , mensajes de correo electrónico o cualesquiera otros documentos". Esta enumeración tiene como nov edad destacable la incorporación de los mensajes de correo electrónico, incluyéndolos plenamente en el concepto de documento.

Igualmente el mismo artículo, en su párrafo segundo se refiere a datos personales "registrados en ficheros o soportes informáticos, electrónicos o temáticos", lo cual confirma la intención del Código de abarcar las nuevas tecnologías, extendiendo a las mismas el concepto documental.

El párrafo cuarto vuelve a reiterar esta concepción al agravar la pena para "las personas encargadas responsables de los ficheros, soportes informáticos, electrónicos o temáticos, archivos registros".

Por tanto, cabe concluir que en esta figura delictiva se observa una clara intención del legislador de extender el concepto documental al documento electrónico extendiendo al mismo la protección penal. Por primera vez se enumeran expresamente los distintos tipos de documento electrónico y la tecnología y los soportes que le sirven de base.

3.2.3.- De la infidelidad en la custodia de documentos (artículos 413 a 416):

El Título XIX del Código Penal, de los delitos contra la administración pública, en su capítulo cuarto trata de la infidelidad en la custodia de documentos y de la violación de secretos. En concreto, los artículos 413 a 416, se ocupan de la infidelidad de la custodia de documentos en el ámbito de las Administraciones Públicas. Las figuras delictivas que contemplan los citados preceptos se pueden reducir a las siguientes:

a) Infidelidad en la custodia en sentido estricto: artículo 413.

> "La autoridad o funcionario público que, a sabiendas, sustrajer e, destruyere, inutilizare u ocultare, total o parcialmente, documentos cuya custodia le esté encomendada por razón de su cargo, incurrirá en las penas de prisión de uno a cuatro años, multa de siete a veinticuatro meses, e inhabilitación especial para empleo o cargo público por tiempo de tres a seis años."

En consonancia con lo manifestado por el profesor Morales Prats y la profesora Rodríguez Puerta en los Comentarios al Nuevo Código Penal[1], podríamos determinar que el objeto de esta figura delictiva es la "correcta preservación y utilización de los medios o inst rumentos", en este caso documentos, "esenciales para el cumplimiento de los fines propios de la adm inistración".

Hoy en día, los documentos generados por medios informáticos y telemáticos en el ámbito de la Administración constituyen un medio esencial para el correcto cumplimiento de sus actividades y fines

Desde esta óptica, no cabe duda que, hoy en día, los documentos generados por medios informáticos y telemáticos en el ámbito de la Administración constituyen un medio esencial para el correcto cumplimiento de sus actividades y fines.

Entre las novedades incorporadas a la redacción de este artículo, en relación con su antecesor (el 364 del Código Penal derogado), destaca la supresión de la referencia "papeles", quedando únicamente la referente a los "documentos". Esta modificación es correcta, a mi entender, dado que, en consonancia con el espíritu del artículo 26, delimita con mayor rigor el objeto sobre el que recae el acto típico. De este modo, el precepto da a entender que lo que pretende es la protección del contenido del documento, independientemente del soporte sobre el que esté registrado, sea un papel o un disquete de ordenador.

El sujeto activo del delito es "la autoridad o funcionario públ ico" que tenga encomendada, por razón de su cargo, la custodia de documentos. Esta figura se destina a castigar, esencialmente, la infracción del concreto deber de custodia que tiene el agente público sobre los documentos que gestione en el desempeño de sus funciones.

La acción típica consiste en sustraer, destruir, inutilizar u ocultar, total o parcialmente, documentos. Nos hallamos aquí ante varios actos alternativos: sólo es necesario realizar uno de ellos para incurrir en el tipo. Su denominador común se encuentra en la desaparición, total o parcial, de un documento para la Administración Pública.

1.- Quintero Olivares, Gonzalo y otros: "Comentarios al nuevo Có digo Penal". Ed. Aranzadi. Navarra, 1996. Pág. 1810.

Un supuesto de hecho de su comisión sobre un documento electrónico, lo encontramos en el caso del borrado de un archivo del sistema informático (el disco duro del ordenador central), previamente copiado, o no, en un soporte ajeno (un disquete) por el funcionario encargado de su custodia.

Tómese en cuenta, en el ejemplo anterior, que si el funcionario se limitara a copiar el archivo sin borrarlo posteriormente no incurriría en este delito. Es necesario que dicho fichero quede inutilizable o ilocalizable para la Administración, aunque sea parcialmente. La simple copia sólo podría ser tipificada, en su caso, como revelación de secretos, a lo sumo.

Otros supuestos de hecho los podemos hallar en la introducción de un virus en el sistema que, si bien no destruye los datos, impida el acceso a los mismos; la conversión de un documento a formato oculto; la introducción de una clave de acceso adicional no conocida por la Administración; el uso de la criptografía[2] para impedir la lectura de los ficheros; etc.

Si el funcionario se limitara a copiar el archivo sin borrarlo posteriormente no incurriría en este delito. Es necesario que dicho fichero quede inutilizable o ilocalizable para la Administración, aunque sea parcialmente

El objeto sobre el que recae la acción típica es el "documento" . En este punto, nos remitimos a lo comentado anteriormente sobre el artículo 26 del Código Penal y la legislación administrativa al efecto.

En cuanto a la culpabilidad, del tenor literal del precepto se desprende que sólo cabe el dolo. No admite por tanto la culpa o negligencia.

Sobre la posibilidad de concursos, hay que tener en cuenta el artículo 198 del Código Penal, el cual sería aplicable en el caso de que los documentos objeto del delito contengan datos sensibles que afecten al derecho a la intimidad personal y familiar y a la propia imagen de los individuos[3].

b) Menoscabo de las barreras de protección del documento electrónico: artículo 414. El supuesto del "password". En su párrafo primero dice:

> "A la autoridad o funcionario público que, por razón de su carg o, tenga encomendada la custodia de documentos respecto de los que la autoridad competente haya restringido el acceso, y que a sabiendas destruya o inutilice los medios puestos para impedir ese acceso o consienta su destrucción o inutilización, incurrirá en la pena de prisión de seis meses a un año o multa de seis a veinticuatro meses y, en cualquier caso, inhabilitación especial para empleo o cargo público por tiempo de uno a tres años."

Esta figura no se destina a la protección directa del documento. Su intención es la de salvaguardar los medios o barreras interpuestos que impiden o limitan el acceso al mismo por personas no autorizadas.

El autor, a tenor de este párrafo, debe ser el funcionario o autoridad que tenga encomendada la custodia de documentos de acceso restringido por razón de su cargo. Prácticamente coincide con el sujeto activo del delito anterior, la única diferencia recae sobre el objeto de la custodia: siendo en el anterior cualquier documento, en la presente figura debe tener además un carácter restringido.

La acción típica es destruir o inutilizar los medios puestos para impedir el acceso al documento reservado o bien consentir en su destrucción o inutilización. En este caso, se equipara expresamente la conducta activa (destruir o inutilizar) con la conducta omisiva (consentir la destrucción o inutilización).

2.- La criptografía es el método utilizado por la informática para codificar los ficheros e impedir su lectura por todo aquél que no posea una "llave" o código de descifrado. Dicha codificación tiene lugar mediante operaciones y algoritmos matemáticos.

3.- Ver a estos efectos la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, BOE 31-10-1992, nº. 262, [pg. 37037]

Como ya he comentado, el objeto sobre el que debe recaer la acción típica no es el documento en sí, sino el medio puesto para protegerlo de cualquier injerencia no autorizada. Es necesario, además, que dicho documento esté previamente declarado como "de acceso restringido" por la autoridad competente.

Como indican Morales Prats y Rodríguez Puerta, dicha acción puede alcanzar "desde la destrucción de una clave informática de acceso a los mismos hasta el quebrantamiento de cerraduras u otras barreras materiales destinadas a impedir el acceso a los documentos".

¿Cabría incluir el caso del password como supuesto de hecho?

Podemos definir el password como la contraseña que, junto a un login o identificación, nos permite el acceso a unos determinados ficheros del sistema informático, restringidos a toda persona que no la conozca. Este sistema sirve de protección a los archivos al impedir que los mismos sean visionados o manipulados por cualquier persona no autorizada para ello. Desde este punto de vista, el password constituye un "medio puesto para impedir el acceso" a documento s restringidos en formato electrónico.

El password constituye un "medio puesto para impedir el acceso" a documentos restringidos en formato electrónico

Por tanto, en mi opinión, toda destrucción o inutilización de dicho password en un sistema informático público, siempre y cuando proteja documentos declarados de acceso restringido, se encuadra plenamente en el tipo delictivo del artículo 414 de Código Penal, en su párrafo primero.

Los llamados hackers o piratas informáticos, como veremos posteriormente al hablar del particular[4], incurren frecuentemente en este delito al destruir o inutilizar los passwords de entrada a sistemas estatales. Baste recordar las recientes incursiones en la red informática restringida del Pentágono de los Estados Unidos[5], que perfectamente podrían reproducirse en nuestro país.

En cuanto a la culpabilidad, sólo se admite la comisión dolosa del acto delictivo. La expresión "a sabiendas" del artículo 414 no deja lugar a dudas.

El párrafo segundo del presente artículo, que prevé la autoría del particular en esta figura delictiva, será objeto de estudio junto al artículo 416 en el último apartado de este epígrafe.

c) Acceso no autorizado: artículo 415.

> "La autoridad o funcionario público no comprendido en el artícu lo anterior que, a sabiendas y sin la debida autorización, accediera o permitiera acceder a documentos secretos cuya custodia le esté confiada por razón de su cargo, incurrirá en la pena de multa de seis a doce meses, e inhabilitación especial para empleo o cargo público por tiempo de uno a tres años."

Este artículo intenta proteger la confidencialidad en el desempeño de la actividad administrativa, en relación con determinados documentos declarados secretos. Por tanto, el núcleo del injusto podemos determinarlo como la violación del secreto.

4.- Epígrafe B.4, El particular como sujeto activo del delito: artículos 414.2 y 416. El supuesto del "hacker", del mismo Capít ulo V (pg. 26 y siguientes).

5.- En abril de 1998 un grupo de hackers de diversas nacionalidades burlaron los sistemas de protección y passwords del Pentágono de los Estados Unidos logrando tener acceso a información militar reservada. La noticia completa puede encontrarse en el artículo "Hackers: Pentagon Archives Vulnerab les" de 17 de abril de 1998 de Associated Press publicado en la página Web de Mercury Center en la dirección de Internet: http://spyglass1.sjmercury.com/breaking/docs/077466.htm.

El sujeto activo no coincide plenamente con el del párrafo primero del artículo anterior. En este caso, dicho sujeto debe custodiar documentos de carácter "secreto" y no sólo "de acceso restringido".

La acción típica es la de acceder o permitir el acceso, sin la debida autorización, a documentos secretos. Vemos, como en el artículo precedente, que el tipo admite tanto una conducta activa como omisiva en la comisión del delito, equiparándose ambas. El objeto de la acción típica es, de nuevo, el propio documento. Se añade además la exigencia de que previamente haya sido declarado como "secreto" por la autoridad competente.

En cuanto al posible concurso con otras figuras, se han de tener en cuenta los artículos 598 a 603 del Código Penal, que serán aplicables cuando el contenido del documento secreto afecte a la defensa nacional.

En cuanto a la culpabilidad, sólo se admite la acción dolosa, tal y como se deriva del término "a sabiendas" utilizado por el artículo 415. No se admite su comisión por culpa o negligencia.

Los únicos sujetos activos admisibles son funcionarios o autoridades públicas. Esto es así a consecuencia de su concreto deber de custodia sobre los documentos públicos

d) El particular como sujeto activo del delito: artículos 414.2 y 416. El supuesto del "hacker"

Los anteriores preceptos estudiados tienen en común que los únicos sujetos activos admisibles son funcionarios o autoridades públicas. Esto es así a consecuencia de su concreto deber de custodia sobre los documentos públicos, en razón del cargo que ocupan dentro de la Administración.

Sin embargo, esta situación encuentra dos excepciones: el artículo 414, párrafo segundo, y el 416 del Código Penal, en los que se atribuye un papel activo al particular. Ésta es su redacción:

Artículo 414, párrafo segundo:

> "El particular que destruyere o inutilizare los medios a que se refiere el apartado anterior será castigado con la pena de multa de seis a dieciocho meses" [6]

Artículo 416:

> "Serán castigados con las penas de prisión o multa inmediatamente inferiores a las respectivamente señaladas en los tres artículos anteriores los particulares encargados accidentalmente del despacho o custodia de documentos, por comisión de gobierno o de las autoridades o funcionarios públicos a quienes hayan sido confiados por razón de su cargo, que incurran en las conductas descritas en los mismos."

Ambos preceptos tienen dos elementos en común:

- La referencia al particular como sujeto activo del delito.
- Una atenuación de la pena en relación con la prevista para el funcionario o autoridad que cometa el mismo acto delictivo.

En cuanto a éste último punto, la atenuación de la pena encuentra su explicación en el menor deber de custodia exigible al particular en relación con los bienes jurídicos de la Administración, dado que no tiene un cargo público que se lo imponga (al menos en el mismo grado que un funcionario de carrera o una autoridad).

6.- Se refiere a los medios de protección del documento comentados en el epígrafe B.2 del mismo Capítulo V (pg.23).

En cuanto al primer punto, la referencia al particular como sujeto activo del delito, ambos preceptos se diferencian en una cuestión que, entiendo, es fundamental:

El artículo 416 exige que dicho particular esté "encargado acci dentalmente del despacho custodia documentos, por comisión de gobierno o de las autoridades su función o funcionarios públicos a quienes hayan sido confiados por razón de su cargo". En este ca so, podemos afirmar que se trata de un particular "revestido" de una función pública, aunque ésta sea accidental, a partir de un ente o persona pública. Por tanto, a mi entender, no se trata de un verdadero particular, en su concepción de "persona totalmente ajena a las funciones públicas", pudiéndose le exigir un mínimo deber de custodia.

El artículo 414.2, en cambio, se refiere al particular sin atribuirle ninguna connotación pública. En este caso, se puede afirmar que nos hallamos ante un verdadero sujeto privado al que no alcanza un concreto deber público de custodia. El mismo Código reconoce tal circunstancia, pues impone una pena inferior en el artículo 414.2, una simple multa, que en el 416, que puede llegar hasta prisión.

¿Cuál es la razón de que el Código Penal contemple este tipo delictivo?

Siguiendo el tenor literal del artículo 414, cualquier individuo podrá incurrir en el delito de destrucción o inutilización de los medios puestos para impedir el acceso a documento restringidos de la administración.

Cualquier individuo podrá incurrir en el delito de destrucción o inutilización de los medios puestos para impedir el acceso a documento restringidos de la administración

En mi opinión, además de cubrir los supuestos de hecho clásicos, esta figura delictiva viene a cubrir una importante laguna punitiva: las actividades de los hackers o piratas informáticos. Los hackers son sujetos con amplios conocimientos informáticos que hacen uso de los mismos para infiltrarse, a través de las redes como Internet, en sistemas informáticos ajenos, preferentemente de grandes empresas o de Administraciones Públicas. Sus motivaciones son variadas: desde las lúdicas o de mero divertimento hasta las ideológicas o políticas, pero nunca por razones económicas o de lucro.

Asimismo, estos individuos no persiguen causar un daño a los documentos a los que accedan ni, generalmente, robar información contenida en los mismos. Su única finalidad es burlar los medios de protección del sistema informático en sí mismos.

Ante esta situación, no existe otro medio de perseguir las acciones de los hackers que no sea el de penalizar la propia destrucción o inutilización de los medios destinados a impedir el acceso a los documentos electrónicos restringidos. A esta razón obedece, desde mi punto de vista, el tipo delictivo contenido en el párrafo 2º del artículo 414 del Código Penal.

Este precepto, por tanto, no penaliza el acceso del hacker a la información reservada, sino únicamente la destrucción o inutilización de los passwords o demás barreras puestas para impedirlo. Sin duda, esta es una nueva clase de delincuencia que puede producir grandes perjuicios en una sociedad cada vez más dependiente de los ordenadores. En otros países como Estados Unidos ya han tenido serios problemas con estas actividades[7]. En España, aún son pocos los casos pero, sin duda, irán en aumento con la implantación y universalización de las nuevas tecnologías, cabe destacar la

7.- Además del caso del Pentágono comentado en la nota nº25, ha habido otros muchos en los Estados Unidos como por ejemplo el producido en febrero de 1998 en el que el FBI arrestó a dos adolescentes que se habían infiltrado en varias redes militares. Otro caso acaeció en la Eglin Air Force Base de Florida, en junio del mismo año, donde consiguieron descubrir a un hacker que intentó acceder a información sobre pruebas de misiles y bombas. (Más información en el artículo: "Los militares estadounidenses inician operaciones contra hackers" e scrito por S.A. Salvador y publicado en la edición del 16 de julio de 1998 del diario electrónico de Noticias Intercom, en la siguiente dirección de Internet: http://www.noticias.com/html/1998/9807/noticias1607.htm

detención de un grupo organizado de hackers, denominado Hispahack, en abril de 1998 en Cádiz y en Asturias, que se habían infiltrado en varios sistemas informáticos españoles y extranjeros[8].

Como comentario final, me permito la observación de que quizás esta figura estaría mejor encuadrada entre los delitos de daños[9], donde la intervención del particular no plantearía tantos interrogantes.

3.2.4.- Registro ilegal de documentos (artículo 534):

El Título XX, De los delitos contra la administración de justicia, Capítulo V, De los delitos cometidos por los funcionarios públicos contra las garantías constitucionales, en su Sección 2ª, De los delitos cometidos por los funcionarios públicos contra la inviolabilidad domiciliaria y demás garantías de la intimidad, trata, en el artículo 534, del registro ilegal de "papeles, documentos o efectos de una persona".

Diferenciación entre los "papeles" y los "documentos" strictu sensu. El concepto de documento se revela más amplio en cuanto a los soportes que admite y más restringido en cuanto a sus requisitos y relevancia jurídica

Cabe destacar, en esta figura, la diferenciación entre los "papeles" y los "documentos" strictu sensu, eludiendo conscientemente la identificación tradicional entre los mismos. El concepto de documento se revela más amplio en cuanto a los soportes que admite y más restringido en cuanto a sus requisitos y relevancia jurídica.

a) Acceso no autorizado o revelación de documentos secretos que afecten a la defensa nacional (artículo 600 y 603):

En el marco del Título XXIII, De los delitos de traición y contra la paz o la independencia del estado, y relativos a la defensa nacional, Capítulo III, De los delitos relativos a la defensa nacional, Sección 1ª, Del descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional, hallamos dos artículos que incorporan como elemento objetivo del tipo el concepto de documento:

El artículo 600 castiga al que "reprodujera planos o documentación referentes a zonas, instalaciones o materiales militares que sean de acceso restringido" y, asimismo, al que "tenga en su poder objetos o información legalmente calificada como reservada o secreta".

El artículo 603 pena al que "destruyere, inutilizare, falseare o abriere sin autorización la correspondencia o documentación legalmente calificada como reservada o secreta (...) que tenga en su poder por razones de su cargo o destino".

En estos preceptos, se exigen tres requisitos fundamentales que debe cumplir el objeto del tipo delictivo:

1.- Ha de ser, necesariamente, un documento.
2.- Debe haber sido declarado como reservado o secreto por la autoridad competente, con arreglo a la ley y con carácter previo a la comisión del hecho.
3.- Su contenido debe afectar a la defensa nacional.

Es necesario, por tanto, que se cumplan las tres condiciones para que sea aplicable esta figura delictiva al supuesto en cuestión. En caso contrario, habría que buscar su penalización mediante su inclusión en otro tipo delictivo.

8.- DRAGO, Mirta: "Hispahack: tres *cerebros* desactivados". Artículo publicado por el diario El Mundo del siglo XXI, en su edición de 4 de abril de 1998.
9.- Dentro del Capítulo IX, de los Daños, del Título XIII, delitos contra el Patrimonio y el Orden Socioeconómico, del Código Penal vigente.

4.- Obtención de pruebas

La obtención de pruebas es una cuestión bastante delicada debido a que podemos estar violando los derechos fundamentales tanto de los usuarios del sistema como de los propios hackers. Normalmente, los mismos medios y mecanismos que son empleados por los autores de la infracción para su perpetración pueden ser utilizados para el esclarecimiento de los hechos y la identificación de los presuntos delincuentes.

Para este supuesto, utilizamos el sniffer SNORT en una SUN SPARC ULTRA I con el sistema SunOS 5.8 Generic February 2000 capturando sólo las IPs que acceden al puerto utilizado por los intrusos y poniendo la fecha y la hora de cada acceso al sistema. Para que no hubiese ningún tipo de error en la captura de la fecha y la hora se utiliza el NTP que está sincronizado con nuestro servidor NTP que a su vez está sincronizado con RedIRIS. Cuando se instale y se retire habrá que hacerlo conjuntamente con la Guardia Civil, así como la posterior extracción y grabación en soporte magnético de los logs.; la Guardia Civil levantará la oportuna Acta a tal efecto.

REGLAS DEL SNORT

```
buscados udp $EXTERNAL_NET any -> $HOME_NET 666 (msg:"[ATENCION-666] Paquete UDP a puerto 666";)
buscados tcp $EXTERNAL_NET any -> $HOME_NET 666 (msg:"[ATENCION-666] Paquete TCP a puerto 666";)
buscados tcp $EXTERNAL_NET any -> $HOME_NET 666 (msg:"[ATENCION-666] Conexion TCP a puerto 666" ; flags:S;)
```

Además en este caso se pudo sacar información de los ficheros de configuración del servidor FTP, así como del robot IRC.

La obtención de pruebas es una cuestión bastante delicada debido a que podemos estar violando los derechos fundamentales tanto de los usuarios del sistema como de los propios hackers

5.- Realización del informe

Para la realización del informe habrá que tener los siguientes puntos en cuenta:

1.- DESCRIPCIÓN DEL CASO. Se documentará de una manera clara y concisa: dónde ha sido el ataque, cómo se ha descubierto, las personas de contacto, quién es el responsable de equipo, para qué se usa, etc.

2.- SISTEMA ATACADO. Donde se describirá: la marca, el modelo, características técnicas del equipo y número de serie. También es importante incluir el coste del equipo y una valoración del coste de la reparación (limpieza del ataque, horas de investigación, etc.) así como de la información que contiene. Además se podrían incluir las vulnerabilidades detectadas especificando el software que se ha usado para dicha detección y en caso de ser de pago se pondrá el número de licencia y su fecha de vencimiento.

3.- DESCRIPCIÓN DEL ATAQUE. Se documentará el ataque explicando sin entrar mucho en detalle cómo entraron, qué han hecho, etc. Una cuestión que se debe comentar son las herramientas que han usado, pero nunca los comandos empleados para acceder al sistema pues nunca se sabe quién puede leerlo y sus intenciones en un futuro.

4.- ANEXOS. Donde se ampliarán los anteriores partes con los ficheros de configuración de las herramientas empleadas, así como las fotos del entorno atacado.

6.- Pasos a seguir por la Guardia Civil

- Recepción de la denuncia por parte de la persona física o jurídica, ya sea por medio de su representante legal (empresas o instituciones), del administrador del equipo informático o de la red. Es importante que el encargado de la puesta en conocimiento del presunto hecho delictivo, tenga una clara y concreta composición del hecho, así como que aporte (si fuese posible) algún tipo de indicio en formato electrónico (disquete, CDRom, zip, etc.), si se aportaran correos electrónicos esto último es muy importante, sin perjuicio de la perceptiva inspección ocular que se hará con posterioridad.

  De la misma forma es conveniente, una valoración aproximada de los daños (en el caso que existan), sin perjuicio de que posteriormente se puedan modificar.

- Minuciosa inspección ocular por parte de la Guardia Civil que le permita analizar todos los indicios, rastros o posibles pruebas que pudiesen existir en el equipo informático, para esto, si fuese necesario, se realizaría una "copia espejo" del disco duro.

  En caso de ser necesario para el proceso penal se precintarían los componentes afectados, procediéndose a su depósito a disposición de la Autoridad Judicial que entendiera de ese hecho; dicho depósito se realizaría en las instalaciones propias del denunciante, siendo éste el que figuraría como depositario. En caso de que el equipo informático fuese necesario para una actividad concreta y necesaria en algún ámbito, se podría poner en normal funcionamiento, haciendo constar este hecho por escrito y siempre debidamente fundamentado. En este caso se deben salvar, como mínimo, las estructuras de los directorios del equipo afectado.

- Realización de un informe complementario para su remisión al juzgado en unión de todo lo actuado, en el que se indicaría de forma clara y lo menos técnica posible el proceso del ataque a ese sistema informático, así como las conclusiones a las que se ha llegado. Este informe puede ir complementado con otros en los que se explique de forma más detallada, huyendo de excesivos tecnicismos, el funcionamiento de algún servicio y/o concepto relacionado con internet (Correo electrónico, números IP, sniffers, etc.)

Minuciosa inspección ocular por parte de la Guardia Civil que le permita analizar todos los indicios, rastros o posibles pruebas que pudiesen existir en el equipo informático

El resto de los pasos, son los característicos en cualquier investigación, hasta el total esclarecimiento de los hechos, así como la puesta a disposición judicial de los presuntos responsables, si fuese el caso.

Agradecimientos

Nos gustaría agradecer a: Luis Martín Velasco (Capitán Jefe UOPJ Pontevedra), Chelo Malagón (RedIRIS), Jesús Sanz (RedIRIS) y Raquel Alcántara (AFYVE) por su inestimable ayuda en todo este caso.

Bibliografía

- http://www.leydatos.com/
- http://www.hispasec.com/
- http://www.rediris.es/
- http://www.virtualey.com/
- http://www.pintos-salgado.com/
- http://www.ipf.uvigo.es/
- http://www.cert.org/

- ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M.: "Los delitos de falsedad y lo s documentos generados electrónicamente. Concepto procesal y material de documento: nuevas técnicas". Cuadernos de Derecho Judicial. La nueva delincuencia II. Consejo General del Poder Judicial. Madrid, 1993.
- ASSOCIATED PRESS: "Hackers: Pentagon Archives Vulnerables". Mer cury Center, 17 de abril de 1998: http://spyglass1.sjmercury.com/breaking/docs/077466.htm
- DAVARA RODRÍGUEZ, M. A.: "El documento electrónico, informático y telemático y la firma electrónica". Actualidad Informática Aranzadi, nº 24, Navarra, julio 1997.
- DAVARA RODRÍGUEZ, M. A.: "Derecho Informático". Ed. Aranzadi. N avarra, 1993.
- DEL PESO, E., PIATTINI, M. G.: "Auditoría Informática", 2ª ed. Ed. RA-MA, 2000.
- QUINTERO OLIVARES, G. y otros: "Comentarios al nuevo Código Pen al". Ed. Aranzadi. Navarra, 1996.
- RIVAS LÓPEZ, J. L., ARES GÓMEZ, J. E., SALGADO SEGUÍN, V. A. y CONDE RODRÍGUEZ, L. E.: "Situaciones de Hackeo [II]: penalización y medidas de segurida d". Ed. PrensaTécnica. Revista Linux Actual nº 15, 2000.
- RIVAS LÓPEZ, J. L., ARES GÓMEZ, J. E., SALGADO SEGUÍN, V. A. y CONDE RODRÍGUEZ, L. E.: "Situaciones de Hackeo [I]: pasos habituales del hacker". Ed. P rensaTécnica. Revista Linux Actual nº 14, 2000.
- RIVAS LÓPEZ, J. L., ARES GÓMEZ, J. E., SALGADO SEGUÍN, V. A y CONDE RODRIGUEZ, L. E.: "Hackers: Procedimientos frente a sus ataques". Ed. Virtualibro .
- RIVAS LÓPEZ, J. L., ARES GÓMEZ, J. E., SALGADO SEGUÍN, V.A. "Li nux: Seguridad técnica y legal". Ed. Virtualibro.
- SANZ LARRUGA, F. J.: El Derecho ante las nuevas tecnologías de la Información, nº 1 del Anuario de la Facultad de Derecho da Universidade da Coruña (1997), pp. 499-516.
- SHELDON, T., COX, P.: "Windows 2000 Manual de seguridad". Ed. O sborne McGraw-Hill, 2002.
- VARIOS: "Seguridad en Windows 2000 Referencia técnica". 1ª ed. Ed. Microsoft Press, 2001.

José Luis Rivas López
(jlrivas@uvigo.es)
A.T.I.C. Universidad de Vigo
Victor Alberto Salgado Seguín
(vsalgado@pintos-salgado.com)
Abogado del bufete Pintos & Salgado
Gonzalo Sotelo Seguín
(gonzasoltelo@guardiacivil.es)
Unidad Orgánica de Policía Judicial
Comandancia de la Guardia Civil de Pontevedra
Pablo Fernández Baladrón
(pablof@uvigo.es)
A.T.I.C. Universidad de Vigo
Servicios Informáticos