Nuevas formas de delinquir

Alberto Alberto Maricel Lucero
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
maricel_bloom@hotmail.com

RESUMEN

Si bien las nuevas tecnologías atrajeron el auge y desarrollo en varias empresas en cuanto a prestación de servicios a la sociedad se refiere, tambien se ha convertido en el nicho de quienes realizaban actos criminales de la manera clásica. En este trabajo describiremos en que consisten estas nuevas formas de delinquir para tener un claro concepto y estar atentos para reconocerlos, tomando medidas en contra de su accionar.

Palabras Clave

Cybercriminalidad, delito informático, espionaje, spyware.

1. INTRODUCCIÓN

La informática despierta con la explosiva incorporación del Internet, que presente en todos los ámbitos del ser humano, revolucionando los patrones de comportamiento y por ende las relaciones sociales.

La obtención es factible mediante el uso de direcciones electrónicas y nombres de dominio, así como la aplicación es cada ves más frecuente del comercio electrónico en tiendas virtuales y empleos de contratos informáticos entre personas naturales y jurídicas.

Tenemos en cuenta que la disciplina del Derecho se halla hoy en día una instancia histórica en la que debe responder a estos nuevos y complejos problemas a los que se enfrenta.

2. EL DELITO INFORMÁTICO

El delito informático implica actividades criminales que los países trataron evitar, tales como robos, hurto, falsificaciones u otras. Sin embargo, el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del Derecho.

El delito informático puede ser considerado como un acto ilegal, no ético o no autorizado que involucra el procesamiento de datos y la transmisión de los mismos.

Existen diversas denominaciones para indicar las conductas ilícitas en las que se usa la computadora para realizar los delitos se podrían mencionar algunos como: delitos Informáticospropiamente dichos, delitos electrónicos, delitos computacionales, crímenes por computadora, delincuencia relacionada con el ordenador, Cyber-crímenes, etc.

3. CYBERCRIMINALIDAD

La criminalidad informática también denominada de cyber-criminalidad puede afectar a bienes jurídicos tal es el caso de delitos en los que se utiliza el computador para redactar una carta difamando a personas físicas o jurídicas, o atentar contra la integridad personal, la fe publica o la seguridad nacional por ello tomamos en cuenta la legislación penal, en el caso de los Bienes Informáticos, consiste en dar facilidad al acceso de datos ha ingresar a la información computarizada, archivos y programas insertos en el soporte lógico del ordenador. En este tipo de conductas se encuentra el espionaje, fraude y el sabotaje informático.

El problema principal era la reproducción no autorizada de programas informáticos y el uso indebido de cajeros automáticos.

Así también los “Delitos Informáticos o ¨cybercrímenes¨, se incluyen a las conductas criminales que, por su gravedad entran en los tipos delictivos.

Es necesario considerar que para una mejor comprensión, aquellas conductas que por su gravedad tiene un tratamiento internacional específico, tales como el fraude informático, robo de software, sabotaje y vandalismo de datos, alteración, acceso y uso indebido de datos informáticos, manipulación informática y parasitismo informático.

Pero solo hablaremos sobre tres de ellos los más frecuentes, se citará únicamente al espionaje, fraude y sabotaje informático.

4. ESPIONAJE INFORMÁTICO

En el Espionaje informático el agente de de los datos computarizados en busca de informaciones sigilosas que posean valor económico. Mencionamos uno de los programas que realizan esa operación spywares.

Estos programas espiones constantemente monitorean los pasos del usuario de un computador conectado a la red de Internet, a fin de trazar un perfil comercial completo.

Tienen la capacidad de apoderarse de informaciones personales del usuario, y son transferidas digitalmente para la sede de una empresa o persona a fin de ser comercializadas, estos programas de espiones tienen la capacidad de enviar informaciones del computador del usuario de la red a desconocidos. Tomando en cuenta que todo digitado hasta el teclado puede ser monitoreado por ellos. Estos tienen el

mecanismo de que cuando un usuario esta en línea o en Internet y baja algún programa y viene con archivo ejecutable spyware; normalmente el usuario no sabe sobre la amenaza de este archivo y lo instala es cuando ya tiene el programa de donde le hacen el espionaje.

Este programa puede obtener informaciones que están en el microcomputador, como las que pasan por el. Utilizan un método de conexión entre propietario y servidor de forma directa e instantánea.

Lo favorable del espionaje informático es que las informaciones se encuentran archivadas en un espacio mínimo y pueden ser transferidas fácilmente a otro soporte similar. Este también puede ser utilizado para producir considerables pérdidas a una empresa u organización, o ser utilizado con fines políticos de tal manera que pudiera atentar contra la seguridad exterior del Estado.

El espionaje informático es considerado como una conducta contraria atentatorio al interés nacional por un gran número de países que pretenden asegurar la protección y seguridad del conglomerado social.

El primer caso en Europa sobre espionaje informático fue en Barcelona - España en 1993 conocido como HISPAHACK. El enjuiciamiento se centra en una actividad que con la expresión anglosajona “Hacking” o “Intrusismo informático” hace referencia a un conjunto de comportamientos mediante los cuales se accede de manera secreta y reservada a un sistema informático, con el fin de causar un perjuicio al titular del bien o a terceros

Se podría decir que la conducta del imputado no es simplemente una intrusión ilegal a un sistema informático, sino la comisión de espionaje informático frustrado, puesto que el culpable dio principio a la ejecución del hecho criminoso.

La defensa, siguiendo el libro sobre los Delitos y las Penas, sostiene que la justicia es sometida a penas ilimitadas y hechos inventados por los, no puede ni debe ser la actual, puesto que la ley previamente estipula los hechos son considerados como delitos y señala de igual manera los límites dentro de los cuales se puede aplicar una pena.

La característica de esta responsabilidad penal propone, como toda responsabilidad jurídica, que el hecho que la genera contravenga a la ley, puesto que nadie puede ser condenado a pena alguna sin que exista una ley anterior que haya definido la conducta como delito y fijado la pena correspondiente, tomando en cuenta el principio de reserva propio del derecho penal.

5. FRAUDE INFORMÁTICO

El fraude informático es conocido como una conducta consistente en la manipulación de datos, alteración o procesamiento de datos falsos contenidos en el sistema informático, realizado con el propósito de obtener un beneficio económico.

Entre estos supuestos se encuentran el Fraude por manipulación de un computador contra un procesamiento de datos, el uso de datos engañosos ¨data diddling¨ y el fraude en el que se realiza la alteración de datos contenidos en el computador antes o durante su proceso informático.

El fraude informático puede cometerse mediante el usote los siguientes: los famosos caballos de Troya, la técnica Salami y el delincuente informático (más conocido como hacker).

Estas acciones criminosas violan la integridad física del propio computador, encontrándose fraudes en el nivel de Entrada o input . Esta conducta, también llamada de manipulación del Entrada o input, revelaría en la conducta del agente el ánimo de alterar datos, omitir o ingresar datos verdaderos o introducir datos falsos en un ordenador.

El delincuente informático modifica los programas en el soporte lógico del ordenador, sin alterar los datos electrónicos existentes. Puede igualmente interferir en procesamiento de la información, alterando solo el programa original o adicionando al sistema.

Fraudes de output es el acto de falsear el resultado inicialmente correcto, obtenido por el ordenador.

6. SABOTAJE INFORMÁTICO

EL sabotaje Informático conocido como el acto mediante el cual se logra inutilizar, destruir, alterar o suprimir datos, programas e información computarizada, sus inicios fue en los laboratorios del Instituto de Masachusetts en 1960, cuando fue creado por primera vez un dispositivo informático destructivo mediante la utilización del lenguaje Assembler.

Su modo operativo es a través de bombas lógicas o cronológicas, bombas de software, virus polimorfos, gusanos, cáncer rutinario, virus de sector de arranque. Un ejemplo representativo de este virus es el “virus Navidad’ que estalla cada 25 de diciembre en el computador infectado, una bomba cronológica puede servir como medio de extorsión para la obtención de un desembolso pecuniario en perjuicio del titular del bien informático, si a cambio la bomba lógica es desactivada.

Estos dispositivos informáticos son también denominados como: tecnovirus, programas criminales y asesinos electrónicos.

Estos destruyen la información en milésimas de segundo

Entre los dispositivos informáticos mas destructivos utilizados para cometer sabotaje informático podemos mencionar a:

Bombas de Software. Estos programas informáticos detonan a pocos minutos de ser introducidos en una red o al ser

cargados en el ordenador. No esperan ninguna condición previa para activarse ni necesitan auto duplicarse.

La diferencia entre las bombas lógicas y las de software es la necesidad de que en las bombas lógicas exista una orden especial por parte del programador para activar la misma con el fin de que explote.

Time bomber. Parecidas en su estructura y funcionamiento a las bombas lógicas, las bombas de tiempo explotan en una fecha determinada. Son considerados programas ocultos destinados a activarse en una fecha memorable. Ejemplo: virus "Navidad", el cual explota solo en fecha 25 de diciembre.

Una forma de evitarlos es adelantando el reloj y ellos no logran ejecutarse.

Cáncer rutinario. Se fabrica en forma análoga al infiltrar al virus mas legítimos de procesamiento de datos o para modificar o destruir los datos, pero este virus no se puede regenerar.

Gusanos electrónicos. Son programas que viajan o se arrastran a través de un sistema informático interconectado borrando toda la información computarizada que encuentre a su paso, se cargan en la memoria de la computadora infectada introduciendo mensajes burlones, causando fallas de operación. Son también denominados "dispositivos informáticos polillas", pues al introducirse en el ordenador destruyen la información borrándola, pudiendo auto replicarse.

Este virus gusano puede dar instrucciones a un sistema informático de una empresa comercial para que le envíe información de sus clientes deudores para posteriormente destruir esa información.

6. CONCLUSIÓN

En conclusión tenemos que el espionaje, fraude y sabotaje de tipo informático son muy peligrosos ya que a causa de estas tres cosas tenemos el riesgo de tener grandes perdidas más que todo de los datos y/o la información privada que se tiene en cada computador (os archivos, documentos y otras cosas de un valor comprensible en algunos casos sólo para su portador), puede resultar penosa e irreversible su recuperación. Es necesario tener conocimiento sobre esto para poder evitarlo y no tener dichas perdidas.

7. REFERENCIAS

[1]ALTMARK, Daniel. Informática y Derecho "Aportes de doctrina Internacional"

[2]AZPILCUETA, Hermilio. Derecho Informático

[3]BALDO DEL CASTANO, Vicente. Conceptos fundamentales del Derecho

[4]http://www.alfa-redi.org/rdi-articulo.shtml?x=7182