DELITOS INFORMÁTICOS: GENERALIDADES

AUTOR: SANTIAGO ACURIO DEL PINO.

NOVIEMBRE: 2016

San Marcos

Introducción

Investigar el delito desde cualquier perspectiva es una tarea compleja; de eso no hay duda. Las dificultades que surgen al tratar de aplicar el método científico a la Delincuencia Transnacional y al Crimen Organizado en buena parte ya fueron establecidas en estudios anteriores, pero enfrentar este tipo de delincuencia a todo nivel es la tarea a la que se ve avocada le Ministerio Público por mandato constitucional y por disposición legal. Ahora bien, el fenómeno descrito en los últimos tiempos ha tenido un avance significativo tomando en cuenta la manifestación de la globalización, la cual no solo ha tenido beneficios, sino también ha contribuido a la masificación de esta clase de delitos y tecnificado a otra clase de cómo son los llamados Delitos Informáticos.

En las páginas siguientes se pretende brindar información en relación a los diferentes delitos informáticos, sus características básicas y el tipo de daño que los mismos ocasionan.

Contenido

Introducción 1
Delitos Informáticos 3
Los fraudes 3
LOS DATOS FALSOS O ENGAÑOSOS 3
MANIPULACIÓN DE PROGRAMAS O LOS “CABALLOS DE TROYA” 3
LA TÉCNICA DEL SALAMI 3
MANIPULACIÓN DE LOS DATOS DE SALIDA 3
El sabotaje informático 4
GUSANOS 4
VIRUS INFORMÁTICOS Y MALWARE 4
CIBERTERRORISMO 4
ATAQUES DE DENEGACIÓN DE SERVICIO 4
El espionaje informático y el robo o hurto de software 4
FUGA DE DATOS (DATA LEAKAGE) 4
REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL 4
El robo de servicios 4
HURTO DEL TIEMPO DEL COMPUTADOR 5
El acceso no autorizado a servicios informáticos 5
LAS PUERTAS FALSAS (TRAP DOORS 5
LA LLAVE MAESTRA (SUPERZAPPING 5
PINCHADO DE LÍNEAS (WIRETAPPING) 5
PIRATAS INFORMÁTICOS O HACKERS 5
Conclusiones y recomendaciones 6
Referencias bibliográficas 6

Delitos Informáticos

A continación se detallan una serie de tipos de delitos Informáticos, de los que la delincuencia se vale para realizar los diferentes ataques a los usuarios individuales o a las organizaciónes.

Los fraudes

LOS DATOS FALSOS O ENGAÑOSOS (Data diddling).
Conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático es conocido también como manipulación de los datos de entrada.

MANIPULACIÓN DE PROGRAMAS O LOS "CABALLOS DE TROYA" (Trojan Horses)
Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

LA TÉCNICA DEL SALAMI (Salami Technique/Rounching Down).
Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada de transacciones financieras y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

MANIPULACIÓN DE LOS DATOS DE SALIDA
Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

El sabotaje informático

GUSANOS

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

VIRUS INFORMÁTICOS Y MALWARE

Son elementos informáticos que, como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro.

CIBERTERRORISMO

Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje.

ATAQUES DE DENEGACIÓN DE SERVICIO:

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a muchos usuarios.

El espionaje informático y el robo o hurto de software

FUGA DE DATOS (DATA LEAKAGE)

También conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa.

REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL

Esto puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales.

El robo de servicios

HURTO DEL TIEMPO DEL COMPUTADOR

Consiste en el hurto de el tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

El acceso no autorizado a servicios informáticos

LAS PUERTAS FALSAS (TRAP DOORS), consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

LA LLAVE MAESTRA (SUPERZAPPING)

Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.

PINCHADO DE LÍNEAS (WIRETAPPING)

Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora. El método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía.

PIRATAS INFORMÁTICOS O HACKERS

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Conclusiones y recomendaciones

A fin de concluir, se estima que con el objetivo mitigar los ataques por parte de la delincuencia en el área de la informática ya sea nacional o internacional, que ya se evidencio en las páginas anteriores, sobre las múltiples formas creadas para delinquir en este campo, se debe contar con asesoría en relación a la seguridad informática. Conocer las técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde esta se encuentra almacenada ya sean estos individuales o conectados a una red frente a posibles ataques accidentales o intencionados, puede hacer la diferencia al momento de protegerse y evitar ser víctimas de este tipo de ataques, pero sobre todo, buscar el equipo profesional pertinente y especialiado en la temática, hace que el usuario o organización posean mayor seguidad en las redes.

Referencias bibliográficas

Santiago Acurio Del Pino. (2016). Delitos informáticos: generalidades. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica