Tendencias de la seguridad informática para los sistemas computacionales

Autor: Marcela Díaz Lule

Tesina presentada para obtener el título de:
Lic. En Sistemas Computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarra

UNIVERSIDAD VASCO DE QUIROGA

LICENCIATURA EN SISTEMAS COMPUTARIZADOS

"TENDENCIAS DE LA SEGURIDAD INFORMÁTICA PARA LOS SISTEMAS COMPUTACIONALES"

TESINA

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN SISTEMAS COMPUTARIZADOS

PRESENTA

Marcela Díaz Lule

ASESOR

Ing. y M.A. Sergio Francisco Barraza Ibarra

CLAVE: 16PSU0014Q

ACUERDO: 95006

MORELIA, MICH., DICIEMBRE DE 2004

INDICE GENERAL

CAPITULO I

INTRODUCCION

La computadoras y los sistemas de información ocupan ahora un sitio especial en las empresas donde facilitan la operación eficiente de oficinas de reservación de aerolíneas, departamentos de archivo clínico en hospitales, funciones de contabilidad y nomina, banca electrónica, sistemas de conmutación telefónica, y así como éstas existen un número sin fin de aplicaciones, grandes y pequeñas. Todas estas aplicaciones requieren, cuando es posible, un buen número de horas hombre.

En la actualidad, para muchas organizaciones, los sistemas de información basados en computadoras son el corazón de las actividades cotidianas y objeto de gran consideración en la toma de decisiones. Aumentar la confiabilidad en la información significa que aquellos que diseñan los sistemas de información tendrán una responsabilidad cada vez mayor de ser capaces, utilizables confiables y, por encima de todo, servir como medio para alcanzar fines sin convertirse en un fin por si mismo.

Con la computadora, los sistemas de red y demás telecomunicaciones en el mundo de las empresas se han facilitado enormemente las transacciones informáticas así como el ordenamiento de los datos. La mayoría de las empresas ya sean de negocios o de servicios tienen la información organizada en Base de Datos.

Hablar de los Hackers y Crackers es hablar de dos fenómenos que le están dando un giro a los avances tecnológicos e informáticos de Internet. Hackers, una palabra que suena en todas las personas que se encuentran interesadas en la informática. Proviene de "HACK" el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy en día es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida. Los Crackers (crack destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etc. Esos son los Crackers, adolescentes inquietos que aprenden rápidamente este complejo oficio. Se diferencian con los Hackers porque no poseen ningún tipo de ideología cuando realizan sus "trabajos". En cambio el objetivo principal de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema

injusto" utilizando como arma el propio sistema. Su guerra es silenciosa pero muy convincente.

Hoy en día los piratas cibernéticos se presentan con un cerebro desarrollado, curiosos y con muy pocas armas: una simple computadora y una línea telefónica. En Internet se pueden producir ataques y esos ataques van en contra de algo medular que es la información, la cual puede sufrir distintos tipos de intromisión para agredirla en su confidencialidad o integridad.

Los diseñadores de sistemas le dan demasiada importancia a las estructuras funcionales del software y hardware pero se olvidan lo más importante que es la seguridad. Un sistema de por si no tiene mucha consistencia si no es atacado por alguien de fuera, en este proceso se demuestra la fuerza. Si el intruso entra es por que existe un error en el diseño. En la mayoría de los casos no se castiga al intruso si no que es contratado por esa misma empresa para proveer la seguridad requerida en futuros ataques. Esta política es perseguida por un buen Hacker.

En este documento trato de mostrar las diferentes denominaciones que se les da a las personas buenas o malas que hacen uso de sus conocimientos adquiridos en un terreno complejo y difícil como es el mundo de las nuevas tecnologías que agrupan la informática y las comunicaciones.

CAPITULO II

ANTECEDENTES

Vivimos en un mundo de códigos, encriptaciones y esto se remonta a la segunda Guerra mundial se cifraban los mensajes, las comunicaciones y convertidos a un puñado de palabras indescifrables que usaban los soldados para enviar mensajes de ataque u ordenes de sus superiores y ya existían quienes descifraban el mensaje del enemigo. Por aquel entonces no se conocían como Hackers y ni pensar que estaban penalizados.

El termino Hackers nació en un momento en que las computadoras eran grandes armatostes como las habitaciones de una casa. En su interior, cientos de cables se caldean al lado de las válvulas de vacío.

En los últimos años la tecnología ha crecido a pasos agigantados, por ejemplo cuando se imaginaba la humanidad que el hombre viajaría al espacio, pondría un pie en la Luna, incrementarían los viajes en aviones comerciales, que podrías hablar con un teléfono portátil a cualquier parte del mundo, que habría máquinas que en un determinado momento podrían suplantar algunas funciones que el hombre realizaba con dificultad, ésta

máquina antiguamente era considerada solo para genios, hombres capaces de descifrar luces que prendían y apagaban como un lenguaje de comunicación entre la máquina y el hombre.

Conforme fue pasando el tiempo la computadora fue más accesible en muchas de sus funciones procesaba datos pero su desventaja es que era muy lenta y mucho muy grandes, a parte estas computadoras sólo las tenían el Gobierno y las universidades.

Con el paso de los años se fue modernizando y actualizando conforme a las necesidades de las personas se creo la PC. Esto contribuyó a un gran adelanto, ya que generó nuevos empleos y muchas ganancias para las empresas involucradas.

Actualmente las empresas grandes, medianas y chicas en fin de todo tipo utilizan la computadora como una herramienta fundamental en las labores cotidianas, sin ella muchas de las empresas no funcionarían igual, habría una lentitud en los procesos y posiblemente existiría un caos en las operaciones comerciales.

En este documento tratar de sentar las bases de lo que es el Hacking y explicar o mostrar los conocimientos de un terreno complejo y difícil como es el mundo de las nuevas tecnologías, tecnologías que agrupa la informática, las comunicaciones y los sistemas.

2.1 Objetivo general:

Analizar a los Hackers y Crackers en su desarrollo dentro de la informática, su influencia de manera positiva y negativa en la era digital.

2.2. Objetivos particulares:

- Diferenciar el termino Hacker y Cracker ya que se tiene un concepto equivocado de ellos.
- Analizar los diferentes tipos de Hackers y Cracker
- Analizar su funcionamiento y algunas capacidades que tienen dentro del medio informático.
- Dar a conocer los diferentes tipos de sanciones y penalizaciones que regulan los órganos y entidades federativas.

2.3. La Nueva Cibersociedad.

La nueva cibersociedad surge a partir de la era de la informática llevada al hogar, esto es así ya que la posibilidad de manejar un ordenador ha aumentado de forma considerable al ser altamente accesible estos equipos. Por otro lado el Internet ofrece grandes posibilidades de explotación de mundos desconocidos y el encuentro con software especifico.

El acercamiento para cualquiera de la tecnología de los bits y las comunicaciones, ha despertado el interés de muchos talentos que son capaces de hacer algo más que escribir un texto. Si conocemos el lenguaje a fondo, podemos hacer mas cosas que escribir o dibujar.

A raíz de la introducción de la informática en los hogares y los avances tecnológicos que esta aporta, ha surgido toda una generación de personajes mas o menos peligrosos que difunden el miedo en la red y las empresas que utilizan este medio para la transmisión de datos.

Los Hackes son el principio y el nivel más alto de toda esta nueva sociedad. Estos poseen mayores conocimientos que el resto de grupos, pero emplean metodología poco agresiva para mostrar sus conocimientos. Los Crackers son probablemente el siguiente escalón y los que son capaces de

Crackear sistemas y romper su seguridad, extendiendo el terror entre los fabricantes y programadores del Software.

A continuación hablare de cada grupo por separado:

Hackers: El primer eslabón de una sociedad "delictiva" según los desarrolladores de sistemas estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en los ordenadores remotos, con el fin de dar a conocer que han estado ahí pero no modifican ni se llevan nada del ordenador atacado.

Normalmente son quieres alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuentemente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad.

Este grupo es él mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

Crackers: Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad de romper

sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.

Para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente a través de la red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers. En la actualidad es habitual ver como se muestran los Cracker de Software de forma gratuita a través de Internet.

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

Lamers: Este grupo es quizás el que más número de miembros posee y son los que mayor presencia tienen en la red. Normalmente son individuos con ganas de hacer Hacking, pero que carecen de cualquier conocimiento. Habitualmente son individuos que apenas si saben lo que es un ordenador, pero el uso de este y las grandes oportunidades que brinda el Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet. Normalmente la posibilidad de entrar en otro sistema remoto o la posibilidad

de girar un grafico en la pantalla de otro ordenador, le fascinan enormemente.

Este es el grupo que más peligro acontece en la red ya que ponen en práctica todo el Software de Hackeo que encuentran en la red. Así es fácil ver como un Lamer prueba a diestro y siniestro un "bombeador de correo electrónico" esto es, un programa que envía miles de mensajes repetidos a los correos electrónicos de otra persona hasta colapsar el sistema y después se mofa autodenominándose Hacker.

Copyhackers: Es una nueva raza solo conocida en el terreno del crackeo de hardware, mayoritariamente del sector de tarjetas inteligentes empleadas en sistemas de televisión de pago. Este mercado mueve al año millones de pesos tan solo en América Latina.

Los Copyhackers divagan entre la sombra del verdadero Hacker y el Lamer. Estos personajes poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello "extraen" información del verdadero Hacker para terminar su trabajo. La principal motivación de estos nuevos personajes, es el dinero.

Bucaneros: Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología. Comparados con los piratas informáticos, los bucaneros solo buscan el comercio negro de los productos entregados por

los Copyhackers. Los bucaneros solo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos "Crackeados" pasan a denominarse "Piratas Informáticos" así puestas las cosas, el bucanero es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de cracking a nivel masivo.

Phreaker: Este grupo es bien conocido en al Red por sus conocimientos en la telefonía. Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad también poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

Sin embargo es, en estos últimos tiempos, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, ya que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y /o emplean la información para su proceso de datos.

***Newbie*:** Es un novato o mas particularmente es aquel que navega por Internet, tropieza con una pagina de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo. Después se baja todo lo que puede y empieza a trabajar con los programas.

Al contrario que los Lamers, los Newbies aprenden el Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

***Script Kiddie*:** Denominados Skid Kiddieo Script Kiddie, son el ultimo eslabón de los canales de la Red. Se trata de simples usuarios de Internet, sin conocimientos sobre Hack o el Crack. En realidad son devotos de estos temas, pero no los comprenden. Simplemente son internautas que se limitan a recopilar información de la Red. En realidad se dedican a buscar programas de Hacking en la Red y después los ejecutan sin leer primero los ficheros Readme de cada aplicación. Con esta acción, sueltan un virus, o se fastidian ellos mismos de su propio ordenador. Esta forma de actuar, es la de un desconocimiento total del tema, lo que lleva a probar y probar aplicaciones de Hacking. Podrían llamarse los "pulsabotones" de la Red. Los Kiddies en realidad no son útiles en el progreso del Hacking.

2.4. El Undeground Final.

Cada vez más jóvenes que se autodenominan Hackers y lo único que hacen es soltar Virus y probar programas de Hacking. Esto confunde a la sociedad y este tipo de personas son algo violentas y adolecen lo material. Disfrutan "fastidiando" al vecino y muestran una cara de brillantes cuando sueltan uno de esos fatídicos Virus o gusano en la Red.

Los buenos Hackers, no son nunca descubiertos y apenas aparecen en la prensa, a menos que sean descubiertos por una penetración en un sistema demasiado seguro. Se debe decir y aceptar que le verdadero Hacker posee el control del mundo.

CAPITULO III

MARCO TEORICO.

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar (y desde donde), es tan importante como saber con que soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos (políticas, capacitación).

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

A esta altura del desarrollo de la "sociedad de la información" y de las tecnologías computacionales, los piratas informáticos ya no son novedad. Los hay prácticamente desde que surgieron las redes digitales, hace ya unos buenos años. Sin duda a medida que el acceso a las redes de comunicación electrónica se fue generalizando, también se fue multiplicando el número de quienes ingresan "ilegalmente" a ellas, con distintos fines. Los piratas de la era cibernética que se consideran como una suerte de Robin Hood modernos y reclaman un acceso libre e irrestricto a los medios de comunicación electrónicos.

Genios informáticos, por lo general veinteañeros, se lanzan desafíos para quebrar tal o cual programa de seguridad, captar las claves de acceso a computadoras remotas y utilizar sus cuentas para viajar por el ciberespacio, ingresar a redes de datos, sistemas de reservas aéreas, bancos, o cualquier otra "cueva" más o menos peligrosa.

Como los administradores de todos los sistemas, disponen de herramientas para controlar que "todo vaya bien", si los procesos son los normales o si hay movimientos sospechosos, por ejemplo que un usuario esté recurriendo a vías de acceso para las cuales no está autorizado o que alguien intente ingresar repetidas veces con claves erróneas que esté

probando. Todos los movimientos del sistema son registrados en archivos, que los operadores revisan diariamente.

3.1 Marco histórico.

Existen 2 versiones distintas del nacimiento de los Hackers.

La primera de estas dice que lo que se empezó a llamar hacking tiene su origen en 1876 cuando Alexander Graham Bell inventó el teléfono. Desde aquel entonces el mundo empezó a cambiar, el extraño aparato logró fama súbita y se expandió rápidamente, ya en 1904 se había extendido por todo el continente norteamericano. A principio de los 60 casi todas las grandes empresas instalaban costosas computadoras que ocupaban habitaciones y hasta edificios enteros. La "Bell Telephone" no fue ajena a esa renovación y los sistemas mecánicos y electromecánicos que habían reemplazados a las operadoras fueron desplazados por estas grandes computadoras que controlaron de allí en adelante el flujo de las comunicaciones. Hasta que un día un técnico de la empresa le contó a un amigo como funcionaban los números de prueba que se utilizaban para chequear las líneas.

Semanas mas tarde Mark Bernay (el alias del amigo en cuestión) divulgo el secreto que, desde entonces, permitió realizar llamados de larga distancia gratis o pagando una comunicación local. En poco tiempo las líneas

de Estados Unidos, se vieron pobladas de phreakers, tal como se llamaban así mismos los seguidores de Bernay.

Phreaker es el término que incluso hoy en día se utiliza para calificar a un pirata de las líneas telefónicas, las cuales utiliza sin pagar o pagando menos de lo que debería. En 1961 se denunció el primer robo de servicio. Allí empezó todo. Las computadoras empezaron a conectarse a los teléfonos y a transmitir datos a través de ellos. Ya en los años 80 se filmó la primera película sobre la piratería electrónica, conocida como "Juegos de guerra". Se fundaron las Bases de datos, sitios electrónicos donde la gente hablaba e intercambiaba datos, sobretodo de hacking. Entre los 70 y 80 se dieron los primeros casos de robo de software e información confidencial de empresas. Es ahí donde se empieza a distinguir entre los Hackers, aquellos que buscan la información e informan sobre los fallos de seguridad del sistema, los Crackers, personajes muchas veces confundidos con los anteriores, que destruyen sistemas, copian información y comercializan con ella.

Por otro lado, los primeros en adjudicarse la definición de Hackers fueron estudiantes del MIT (Massachussets Institute of Technology), en su mayoría miembros del Tech Model Railroad Club (TMRC, Club de Modelos de Trenes) que en 1959 se inscribieron en el primer curso de programación que la institución ofreció a sus alumnos. Los computadores de ese entonces, eran unos aparatos demasiado caros que ocupaban salas enteras y

necesitaban una gran carga de suministro eléctrico para funcionar, por lo que el acceso a éstos estaba realmente restringido para los estudiantes, por lo tanto, pocas ocasiones era el usuario final el que manejaba la computadora directamente, sino que habitualmente se veía obligado a dar sus programas a los operadores, que a su vez se encargaban de introducirlos en la computadora y de devolverle los resultados después.

Frente a esta situación, estos estudiantes del MIT, se las ingeniaban para que les dejaran introducir directamente programas a ellos mismos usándolo por las noches desde una sala de terminales a la que en realidad no tenían acceso de modo oficial. Poco tiempo después de aquel curso llegó al MIT el TX-0, una computadora revolucionaria para la época, y el grupo del MIT tuvo la suerte de que Jack Dennis, un antiguo miembro del TMRC y ahora profesor del MIT, les diera acceso prácticamente ilimitado a esa máquina. Para ellos, una de las principales ventajas que tenía ésta era que en lugar de interactuar con los usuarios mediante tarjetas perforadas, tenía un teclado gracias al cual era posible trabajar directamente con él, lo que les permitía ver directamente el resultado de su trabajo, con lo que cada vez empezaron a pasar más y más tiempo con la computadora y pronto eran capaces de hacer cosas con ella que ni sus diseñadores hubieran creído posibles. Fue en éste entorno y en ese momento cuando el término Hacker se empezó a aplicar a aquellos "eruditos" de la informática capaces de hacer maravillas con un computador.

La contribución más importante de este grupo de Hackers a la historia de la informática no fue la de adoptar ese término sino la de ser los primeros en pensar diferente acerca de cómo se usaban las computadoras y de lo que se podía hacer con ellos, y, sobre todo, la creación de una ética que regía su comportamiento que aún sigue vigente hoy en día y que todos los Hackers siguen en mayor o menor medida, sobre todo en la parte que mantiene que la información debe ser libre.

La hazaña que marcó e instaló el término Hackers en el mundo fue cuando el 15 de enero de 1990, la central de larga distancia AT&T se vino abajo, dejando fuera de servicio a miles de abonados. Esto denota cierto interés por las catástrofes creadas por algunos Hackers, más que por sus conocimientos.

De aquí en adelante se reconoce la existencia de un árbol genealógico de los Hackers más famosos, que de alguna manera han marcado la historia.

Hacker es una palabra de origen inglés que significa "cortador" (Hack: cortar) pero que en actividad informática tiene dos significados que, si bien

pueden coincidir en cuando al medio de acceso a la información, los objetivos son distintos.

Según alguna opinión la actividad del Hacker consiste en interceptar en forma dolosa un sistema informático para apoderarse, interferir, dañar, destruir, conocer, difundir o hacer uso de la información que se encuentra almacenada en los ordenadores pertenecientes a instituciones públicas y privadas, de seguridad, entidades financieras y usuarios particulares.

Otra definición más menos agresiva los cataloga como "auténticos genios de la informática", entran sin permiso en ordenadores y redes, averiguan, rastrean y a veces, dejan tarjetas de visita. Los Hackers, posmodernos corsarios de la red, son la última avanzada de la delincuencia informática de este final de siglo".

En la revista especializada PC USER tratan, con fundamentos éticos y filosóficos, cual es la diferencia entre el que utiliza los recursos informáticos para causar daño y los que hacen uso de ellos a solo efecto de romper las barreras del conocimiento.

Según dicha publicación el CRAKER es la persona que ingresa ilegalmente a un sistema informático para robar o destruir información o simplemente para causar desorden. También se llama Cracker a quien descifra los esquemas de protección anti-copia de los programas comerciales

para así poder utilizar o vender copias ilegales. La misma edición cataloga a los HACKERS con cinco acepciones, definiendo la primera como personas que disfrutan investigando detalles de los sistemas operativos y los programas, buscando nuevas formas de aumentar sus capacidades.

En el sitio THE HACKER FAQ (www.solon.com), citado por la misma publicación, "se dice que los Hackers no son aquellos que violan la seguridad de los sistemas. Estos son los Crackers. Los Hackers disfrutan jugando con las computadoras. Pasan mucho tiempo observando un sistema para saber todo sobre él, sobre sus medidas de seguridad. Pero no lo hacen con malicia, sino por simple seguridad".

Según esta última definición el accionar de un Hacker no es robar, sino obtener información sobre un sistema. El problema surge cuando esa información o acceso a la misma, es restringida. En este caso, el Hacker no admite limitaciones y procurará traspasar todas las barreras por medio de técnicas denominadas por ellos mismos como "ingeniería social" que consiste en utilizar cualquier medio informático para acceder a las claves de acceso de cualquier fuente de información.

3.2 Marco Conceptual.

El Internet: De todos es bien sabido que el Internet no es el lugar más seguro. Hoy por hoy, la red de redes contiene mas virus, exploits, comandos java "especiales" y otras especias que paginas WEB existen. Es una paradoja, pero lo cierto es que tienen que andar con cuidado en la red. Los canales IRC suelen estar infectados de "aprendices" que emplean todo tipo de "armamentos" IRC para fastidiar a cuantos chatean en el canal.

El correo electrónico también se ve perjudicado ya que se puede encontrar un mensaje sin sentido que lo único que ha hecho es colocarte un "troyano" en tu computadora o quizás una Virus. El navegar sin precaución por estas paginas, puede resultar peligroso, ya que a veces cuando se hace una descarga de algún programa, este contiene un virus o un troyano.

El pago electrónico a través de la res también esta en peligro, ya que existen programas específicos para interceptar las transiciones o en el peor de los casos emplean el número de tarjeta para futuras compras ajenas.

También existen utilidades que permiten escanear los puestos de cualquier ordenador conectado a la res y utilidades que controlan todos los paquetes que viajan por la red, sin embargo también es cierto que se puede navegar, a menudo, por la red sin tener problemas.

Mailbonbing: Es el envió masivo de correo electrónico comúnmente conocido como bombardeo en el entorno del Hacking. Los Mailbonbing son programas que permiten enviar miles de veces el mismo mensaje a una determinada dirección de correo electrónico.

A veces el mailbombing, tan bien permite el envió de correos fantasmas, esto es, correo falso sin dejar rastro para quien lo envía, esto le permite pasar inadvertido. A esto se le llama correo anónimo.

Cracker: Diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros ordenadores remotos. Muchos crackers "cuelgan" paginas WEB por diversión o envían a la red su última creación de virus polimórfico.

También existen crackers que se dedican a crear Cracks para software importante y negocia con ellos, existen cracks para tarjetas, Shareware y sistemas electrónicos como el DVD o las consolas Playstation entre otros.

IRC: Comúnmente conocido como canal de chateo o "formad e intercomunicarse con otros usuarios en tiempo real a través de texto y ahora

voz" se ha convertido en un canal de guerra en el que entras para preguntar algo en concreto y recibes como respuesta una bomba lógica o un virus.

Existen multitud de herramientas IRC en las paginas de Hackeo y utilidades WAR o de guerra, es una moda ir fastidiando por este canal.

Troyano: Un troyano posee diversos significados y acometidos. Atrás, era un programa oculto que proporcionaba un cuadro de dialogo falso que de debías aceptar, tras lo cual, el troyano se "queda" con lo que tecleabas después, es este caso la clave. Después el troyano encintaba la clave y se enviaba de forma autentica a un correo electrónico especifico, cuando emplea el correo electrónico, sea cual sea la dirección.

Bomba Lógica: Es lo mas parecido a un virus. Una bomba lógica es un programa autoejecutable que espera un determinado tiempo o actividad sobre el teclado para explotar, o dicho de otra manera, infectar el ordenador, modificando textos, mostrando gráficos o borrando parte del disco duro.

Firewall: Un firewall es una utilidad o herramienta de seguridad, que impide que ciertos comandos o paquetes de datos "anormales" penetren en nuestro sistema. Comúnmente son traducidos como barras de fuego, que

detectan ataques o entradas forzadas en los puestos de nuestro sistema. Denominados también nuke.

Pirata Informático: es comúnmente confundido con un Hacker, un pirata informático es quien hace copias de software en CD y comercializa con ellos. No posee conocimientos, más que para duplicar discos y este es el grupo que más ensucia a la nueva sociedad de hackers después de los Lamers.

3.3 Herramientas imprescindibles para el "Hacker"

El Hacker necesita herramientas que le faciliten el trabajo en la red. Entre estas herramientas destacan los escaneadotes y programadores de tarjetas inteligentes. Para entrar en sistemas ajenos, "aunque sea solo para ver dentro de el y salir después" el Hacker debe echar mano a un buen diccionario para obtener la clave de acceso.

Pero lo más importante es la motivación y la intuición, sin ellas nada puede hacer.

Escaneadotes: El más conocido es el Scanerport y como su nombre lo indica, se trata de programas que permiten rastrear la red en busca de

puestos abiertos por el cual acceder y manipular un sistema o introducción de un troyano o virus.

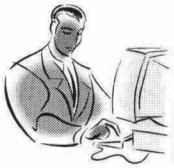
Diccionarios: Existen varios tipos de diccionarios entre la comunidad de Hacker y son imprescindibles dado su contenido. El diccionario de palabras, cuando se emplea la fuerza bruta para obtener los Paswords o contrapesas de un programa, pagina WEB u ordenador remoto, es necesario y muy habitual emplear este diccionario, normalmente en formato de Software.

El programa y /o diccionario electrónico compara miles de palabras hasta dar con la clave correcta, a esto se le denomina fuerza bruta ya que se comparan miles de palabras en menos de un segundo..

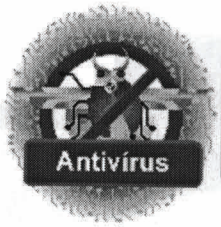
Ingeniería Social: Es quizás la base de un Hacker, para obtener los datos o lo que le interesa por medio de una conversación y de personas. Es la forma de engañar al otro, haciéndole creer que es alguien bueno. Una muestra de ello es el timo de telefónica, en el que te llaman haciéndose pasar por un técnico de la compañía y te solita que teclees un numero después de colgar. Este comando llamado ATT, le permite al ingeniero social, realizar llamadas a través de tu teléfono.

Hackers

BUENOS



1.-Si la vulnerabilidad es descubierta por un Hacker "Write hat", éste normalmente da aviso a la empresa creadora del programa



2.-Una vez alertado, el fabricante suele liberar un "parche", es decir, un programa gratuito que repare la vulnerabilidad.

4.-Existen foros de discusión y listas de correos electrónicos donde se discuten las vulnerabilidades.

5.-Cuando el problema es público, las empresas antivirus empiezan a liberar actualizaciones para sus programas,

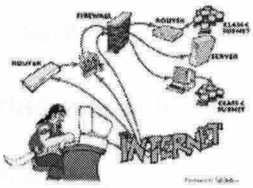
6.-La comunidad "White hat" suele liberar herramientas gratuitas para ayudar a contener los virus mas peligrosos,

7.-Las computadoras que cuentan con los parches y antivirus actualizados difícilmente son infectadas.

VS. MALOS

1.-Cuando el descubridor es un "black hat" generalmente aprovecha la falta para crear un virus o troyano, que libera en el Internet.

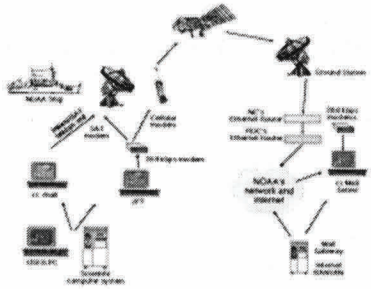
2.-Normalmente la vulnerabilidad se hace pública poco después, conforme el virus se extiende.



4.-Los "black hat", crean inclusive, las llamadas Herramientas de creación de virus y crear cadenas.

5.-Los cibernautas conocidos como Script Kiddies aprovechan las herramientas para crear nuevas variantes de virus.

6.-Los programas maliciosos se extienden por Internet por correo electrónico, mensajerilla instantánea y conexión directa,



CAPITULO IV

MARCO JURÍDICO.

En México no está exento de formar parte de los países que se enfrentan a la proliferación de estas conductas ilícitas. Recientemente, la prensa publicó una nota en la que informaba sobre las pérdidas anuales que sufren las compañías fabricantes de programas informáticos, las que se remontaban a un valor de mil millones de dólares por concepto de piratería de estos programas.

Esto, a la larga podría traer implicaciones muy desventajosas para México, entre las que podemos citar: la pérdida de prestigio a nivel internacional por el actuar ilícito de empresas cuyo radio de acción no está reducido al ámbito nacional y la pérdida de credibilidad por parte de las compañías proveedoras de programas informáticos, lo que se traduciría en un mercado poco atractivo para ellas que pondrían al país en una situación marginada del desarrollo tecnológico.

En este entendido, consideramos que por la gravedad de la conducta ilícita en sí, y las implicaciones que traería aparejadas, justifica su regulación penal.

4.1. Código Penal Federal

Titulo noveno revelación de secretos y acceso ilícito a sistemas y equipos de informática

Capitulo I.- Revelación de Secretos

Artículo 210.- se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.

Artículo 211.- la sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado publico o cuando el secreto revelado o publicado sea de carácter industrial.

Articulo 211 bis.- a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicaran sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.

Capitulo II.- Acceso Ilícito a Sistemas y Equipos de Informática

articulo 211 bis 1.- al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Articulo 211 bis 2.- al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del estado, protegidos por algún

mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Articulo 211 bis 3.- al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

Articulo 211 bis 4.- al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Articulo 211 bis 5.- al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este articulo se incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Articulo 211 bis 6.- para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el articulo 400 bis de este código.

Artículo 211 bis 7.- las penas previstas en este capitulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

4.2. Norma Oficial Mexicana

Es responsabilidad del Gobierno Federal procurar las medidas que sean necesarias para garantizar que los servicios que se comercialicen en territorio nacional contengan los requisitos necesarios, con el fin de garantizar los aspectos de información para lograr una efectiva protección del consumidor;

4.3. Tratado de Libre Comercio de América del Norte (TLC)

Este instrumento internacional firmado por el Gobierno de México, de los Estados Unidos y Canadá en 1993, contiene un apartado sobre propiedad intelectual, a saber la 6a. parte capítulo XVII, en el que se contemplan los derechos de autor, patentes, otros derechos de propiedad intelectual y procedimientos de ejecución.

En términos generales, puede decirse que en ese apartado se establecen como parte de las obligaciones de los Estados signatarios en el área que se comenta que deberán protegerse los programas de cómputo como obras literarias y las bases de datos como compilaciones, además de que deberán conceder derechos de renta para los programas de cómputo.26

De esta forma, debe mencionarse que los tres Estados Parte de este Tratado también contemplaron la defensa de los derechos de propiedad intelectual (artículo 1714) a fin de que su derecho interno contenga procedimientos de defensa de los derechos de propiedad intelectual que permitan la adopción de medidas eficaces contra cualquier acto que infrinja los derechos de propiedad intelectual comprendidos en el capítulo específico del tratado.27

En este orden y con objeto de que sirva para demostrar un antecedente para la propuesta que se incluye en el presente trabajo, debe destacarse el contenido del párrafo 1 del artículo 1717 titulado Procedimientos y Sanciones Penales en el que de forma expresa se contempla la figura de piratería de derechos de autor a escala comercial.

La ley e incluso los medios escritos, aluden a esta nueva generación como aquellos que lindan con lo ilegal. En la actualidad, al fin, se describe a estos personajes como auténticos expertos en sistemas digitales que disfrutan explorando sistemas y probando sus capacidades en oposiciones los simples usuarios, que se conforman con redactar unas cuentas líneas en el procesador de textos.

4.4 Sanciones y medidas de seguridad que prevé el Código Penal del Estado de Michoacán.

El artículo 23 del Código Penal del Estado de Michoacán, establece "Las consecuencias jurídicas del delito son:

- Esencia con trabajo obligatorio;

- Confinamiento;

- Prohibición de ir a lugar determinado o de residir en él;

- Multa;

- Reparación del daño;

- Inhabilitación, suspensión y privación de derechos;

- Destitución y suspensión de funciones o empleos;

- Publicación especial de sentencia;

- Decomiso de los instrumentos del delito;

- Decomiso o destrucción de cosas peligrosas o nocivas;

- Amonestación;

- Apercibimiento;

- Caución de no ofender;

- Vigilancia de la autoridad;

- Internación;

- Intervención, prohibición de realizar determinadas operaciones o negocios, y disolución de las personas jurídicas colectivas; y,

- Tratamiento en libertad, semiliberación y trabajo en favor de la comunidad.

Sanciones.

La prisión consiste en la privación de la libertad corporal y su duración será de tres días a cuarenta años, conforme a la penalidad establecida por el tipo penal correspondiente y se atenderá impuesta con trabajo obligatorio por todo el tiempo de su duración. Se extinguirá en los establecimientos que al efecto señale el Ejecutivo del Estado de acuerdo a la Ley de Ejecución de Sanciones Privativas y Restrictivas de Libertad. En toda sentencia que imponga pena de prisión, se computara el tiempo de detención. los procesados sujetos a prisión preventiva y los reos políticos serán recluidos en establecimientos o departamentos especiales.

Confinamiento.

El confinamiento consiste en la obligación de residir en lugar determinado y no salir de él. No podrá exceder de cinco años. El órgano ejecutor de sanciones hará la designación del lugar, conciliando las exigencias de la tranquilidad pública con las circunstancias personales del sentenciado. Cuando se trate de delitos políticos la designación será hecha por el tribunal que dicte la sentencia.

Multa.

La multa consiste en la sanción económica que se impone al delincuente y se cubre en favor del Fondo Auxiliar para la Administración de Justicia del Estado. Se hará efectiva por conducto de la Dirección del Fondo Auxiliar, tomando su importe de la caución otorgada en autos, o en su caso, por medio del procedimiento económico-coactivo. Las multas especificadas en días de salario, el mínimo general vigente en el momento y lugar en que se cometa el delito. Cuando el sentenciado no pudiere pagar la multa o solamente pudiera pagar parte de ella, el juez fijará en sustitución los días de prisión que correspondan según las condiciones económicas del reo, no excediendo de dos meses.

Reparación del daño.

La reparación del daño comprende:

La restitución de la cosa obtenida por el delito y sus frutos, y si no fuere posible, el pago del precio correspondiente.

El resarcimiento del daño material y moral causado, incluyendo el pago de los tratamientos curativos que, como consecuencia del delito, sean necesarios para la recuperación de la víctima; y,

La indemnización de los perjuicios ocasionados.

La reparación del daño que deba ser hecha por el delincuente tiene carácter de sanción pública. Cuando la reparación sea exigible a terceros, tendrá carácter de responsabilidad civil y se podrá reclamar en forma conexa a la responsabilidad penal o con exclusión de ésta. La reparación del daño material será fijada por los jueces según el que sea preciso resarcir tomando en consideración las pruebas obtenidas en el proceso. Por tener el carácter de pena pública la reparación del daño. El juez debe condenar al acusado a la reparación de ésta lo solicite o no el Ministerio Público, aunque no se demuestre la capacidad económica del obligado a cubrirla.

En orden de preferencia tienen derecho a la reparación del daño:

- El ofendido;

- El cónyuge, los hijos menores de edad y mayores incapacitados;

- Los que dependían económicamente del ofendido; y,

- Sus herederos.

Están obligados a reparar el daño:

- El delincuente;

- Los ascendientes, por delitos cometidos por sus descendientes que estén bajo su patria potestad;

- Los tutores y los custodios, por los delitos de los incapacitados que se hallen bajo su autoridad;

- Los directores o propietarios de internados, colegios o talleres que reciban en su establecimiento discípulos o aprendices menores de 16 años, por los delitos que ejecuten éstos durante el tiempo que se hallen bajo el cuidado de aquellos;

- Las personas físicas, las jurídicas y las que se ostenten con este último carácter, por los delitos que cometa cualquier persona vinculada con

aquellas por una relación laboral con motivo y en el desempeño de sus servicios;

- Las personas morales, o que se ostenten como tales, por los delitos de sus socios, gerentes o administradores, y en general por quienes actúen en su representación. Se exceptúa de esta regla a la sociedad conyugal, pues cada cónyuge responderá con sus bienes propios de la reparación del daño que origine su conducta delictiva;

- Los dueños de mecanismos, instrumentos, aparatos, vehículos o sustancias peligrosas, por los delitos que en ocasión de su tenencia, custodia o uso, cometan las personas que los manejen o tengan a su cargo; y,

- El Estado y los Municipios subsidiariamente, por sus funcionarios y empleados, cuando el delito se cometa con motivo o en el desempeño de sus funciones.

La reparación del daño será hecha, sin afectar los derechos sobre alimentos de las personas que dependan económicamente del delincuente. La reparación del daño se cubrirá con los bienes del responsable y subsidiariamente con el importe de la caución que se otorgue para que aquel obtenga su libertad provisional, o el beneficio de la condena condicional, en caso de que se haga efectiva, o se sustraiga a la acción de la justicia. Si lo anterior no es suficiente, el reo seguirá obligado a pagar el saldo insoluto.

Si las personas que tienen derecho acreditado a la reparación del daño renuncian a ella, su importe se aplicará en favor del estado.

La autoridad judicial, tratándose del pago de la reparación del daño, podrá fijar plazos y autorizar pagos parciales, siempre que el término señalado no exceda de un año. En cuanto a la multa, será la autoridad administrativa encargada de su cobro, la facultada para establecer los plazos que estime convenientes.

Decomiso de instrumentos, objetos y productos del delito.

Los instrumentos del delito, así como las cosas que sean objeto o producto de él, se decomisarán si son de uso prohibido. Si son de uso lícito, se decomisaran cuando el delito sea intencional. Si pertenecen a un tercero, solo se decomisarán cuando el tercero que los tenga en su poder o los haya adquirido bajo cualquier título, esté en el supuesto del artículo 17 fracción V de éste Código. Las autoridades competentes procederán al inmediato aseguramiento de los bienes que podrían ser materia del decomiso, durante la averiguación previa o en el proceso. Se actuará en los términos previstos por este Párrafo cualquiera que sea la naturaleza de los instrumentos, objetos o productos del delito.

Si los instrumentos o cosas decomisados son sustancias nocivas o peligrosas se destruirán a juicio de la autoridad que esté conociendo del caso, pero aquella, cuando lo estime conveniente, podrá determinar su conservación para fines de docencia o investigación. Respecto de los instrumentos del delito o cosas que sean objeto o producto de él, la autoridad competente determinará su destino.

Los objetos o valores que se encuentren a disposición de las autoridades investigadoras o judiciales, que no hayan sido decomisadas y que no sean recogidas por quien tenga derecho a ello en un lapso de noventa días naturales, contados a partir de la notificación al interesado, se enajenarán en subasta pública y el producto de la venta se aplicará a quien tenga derecho a recibirlo.

Si el notificado no se presente dentro de los seis meses siguientes a la fecha de la notificación, el producta de la venta se destinará al mejoramiento de la Procuración o Administración de Justicia. La notificación se hará por una sola vez, mediante edictos publicados en el Diario Oficial del Estado y en el diario de mayor circulación en la entidad.

Amonestación.

La amonestación consiste en la advertencia que el juez hace al sentenciado, en diligencia formal, explicándole las consecuencias del delito que cometió, exhortándolo a la enmienda y previniéndolo de las sanciones que se le impondrían en caso de reincidencia. La amonestación se hará en privado o públicamente, a juicio del juez.

Apercibimiento y caución de no ofender.

El apercibimiento consiste en la comunicación que el juez hace al acusado, cuando se tema fundadamente que está en disposición de cometer un nuevo delito, ya sea por su actitud o por amenazas, de que en caso de cometer el que se propone u otro semejante, será considerado como reincidente.

Cuando los jueces estimen que no es suficiente el apercibimiento, exigirán además al acusado una caución de no ofender.

La caución de no ofender consiste en la garantía que el juez puede exigir al sentenciado, en los casos que estime conveniente, para que no cause un nuevo daño al ofendido. Si el sentenciado prueba que no puede otorgar la garantía, el juez la sustituirá por vigilancia de la autoridad.

Suspensión, privación e inhabilitación de derechos.

La suspensión consiste en la pérdida temporal de derechos, funciones, cargos, empleos o comisiones. La privación es la pérdida definitiva de los mismos. La inhabilitación implica una incapacidad legal temporal o definitiva para obtener y ejercer aquellos.

La suspensión de derechos se origina:

- Por ministerio de la ley, si es consecuencia necesaria de otra sanción: y,

- Por imponerse como sanción independiente.

En el primer caso, la suspensión comienza y concluye con la sanción de que es consecuencia.

En el segundo caso, si la suspensión no va acompañada de sanción privativa de la libertad, se empezará a contar desde que cause ejecutoria la sentencia que la impone y, caso contrario, comenzará al quedar compurgada la sanción privativa de la libertad.

La sanción de prisión suspende los derechos políticos y los de tutor, curador, apoderado, defensor, albacea, perito, depositario, interventor judicial o en quiebras, síndico, árbitro y representante de ausente. La suspensión principiará desde que cause ejecutoria la sentencia respectiva y durará todo el tiempo de la condena.

Publicación especial de sentencia.

La publicación especial de sentencia, consiste en la inserción total o parcial de ella en uno o dos periódicos que circulen en la localidad, los cuales serán escogidos por el juez, quien resolverá la forma en que deberá hacerse. Los gastos originados por tal motivo serán por cuenta del Estado si el juez estima pertinente la publicación, pero si lo piden el sentenciado o el ofendido éstos cubrirán el gasto respectivo.

El juez podrá, a petición y a costa del ofendido, ordenar la publicación de la sentencia en entidad diferente o en algún otro periódico.

La publicación de sentencia podrá ordenarse igualmente a petición y a costa del sentenciado cuando éste fuere absuelto, el hecho imputado no constituya delito o él no lo hubiere cometido.

Si el delito por el que se impuso la publicación de sentencia, fue cometido por medio de la prensa además de la publicación, se hará también en el periódico empleado para cometer el delito, con el mismo tipo de letra, igual color de tinta y en el mismo lugar. El juez tomará en estos casos las

medidas necesarias para que la sentencia referida se publique en forma efectiva.

Legislación nacional.

Para el desarrollo de este capítulo se analizará la legislación que regula administrativa y penalmente las conductas ilícitas relacionadas con la informática, pero que, aún no contemplan en sí los delitos informáticos en este entendido, consideramos pertinente recurrir a aquellos tratados internacionales de los que el Gobierno de México es parte en virtud de que el artículo 133 constitucional establece que todos los tratados celebrados por el Presidente de la República y aprobados por el Senado serán Ley Suprema de toda la Unión.

Sujetos del delito.

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas

informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que los diferencia entre sí, es la naturaleza de los delitos cometidos.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos, el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", los estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros".

Asimismo, dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no son de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas. (6)

CAPITULO V

CONCLUSIÓN Y RECOMENDACIONES

Durante la presente investigación se observó los pocos conocimientos que tienen los usuarios finales sobre el tema, esto es realmente alarmante porque cualquier persona no importa el sexo o edad es vulnerable a los ataques de estos fenómenos, con el simple hecho de estar conectado a la red de redes (Internet) puede ser un blanco facil.

Las tecnologías evolucionan y con ellas los Hackers ya que es un juego en la red, existen virus cada vez más resistentes y a su vez se diseñan sistemas que desean combatir este mal, creando paredes de fuego (firewalls) que combatan contra este tipo de ataques.

Las recomendaciones mas apropiadas para evitar este tipo de ataques en la red son:

- Tener un buen programa de antivirus, que este actualizado y con las herramientas necesarias para resistir cualquier ataque.
- Prevenir que ninguna persona ajena a la empresa o institución tenga acceso alguna máquina y mucho menos al servidor o servidores de la misma.
- Evitar abrir cualquier tipo de programa o correo electrónico de dudosa procedencia ya que esta es la principal causa de ataques de hackers.
- Al momento de detectar cualquier problema con el sistema operativo y/o programas de la maquina en uso, se tiene que reportar al encargado de sistemas de la misma empresa o institución para análisis del mismo y no provocar daños mayores.

BIBLIOGRAFIA

Análisis y Diseño de Sistemas de Información

James A. Senn

McGraw-Hill

Segunda Edición

1992

Constitución Política del Estado de Michoacán.

Cuadernos Michoacanos de Derecho.

Edit. Abz.

Internet y derecho en México.

Barrios Garrido Gabriela, Muñoz de Alba Marcia, Pérez Bustillos Camilo.

Edit. Mc Graw Hill.

México 1998.

Pp.180.

Seguridad informatica para la empresa y particulares.

Álvarez Marañón Gonzalo.

Edit. Mc Graw Hill.

México 2004.

Segunda Edición.

Black ice: La Amenaza del Ciberterrorismo.

Verton, Dan.

Edit. Mc Graw Hill.

España 2003.

Primera Edición.

Claves Hackers.

Horton, Mike.

Edit. Mc Graw Hill.

2004.

Primera Edición.

Firewalls (Manual de Referencia).

Strassberg, Keith E.

Edit. Mc Graw Hill.

España 2003.

Primera Edición.