Seguridad en Sistemas Computacionales

Introducción.

El progreso de la informática y la computación han hecho que nuestra vida en estos últimos años sea cada vez más fácil, permitiéndonos comunicarnos a kilómetros de distancia en sólo segundos y lograr muchos descubrimientos que, gracias a ella, se han podido realizar, siendo herramientas muy importantes en nuestros días. Pero como nada es perfecto, también tiene sus desventajas, ya que, el mundo actual está dependiendo mucho de estas herramientas, y al ser ésto así, es muy fácil que gente con malas intenciones intente, haciendo jugarretas dañar los sistemas y provocar que prácticamente "el mundo se detenga", estos personajes son los crackers, muchas veces confundidos con los hackers y que dañan los computadores mediante códigos que alteran los funcionamientos de las computadoras, que son los virus los cuales, de acuerdo a diversas características se dividen en muchas clases más, dejando al mundo muy preocupado por el daño que pueden realizar.

Pero el mundo no se ha quedado de brazos cruzados, ya que, ingenieros, programadores y muchas personas ligadas al tema han puesto su conocimiento creando Antivirus, Firewalls, además de legislaciones contra delitos informáticos para así minimizar el daño de los virus y a la vez darle una lección a los que se divierten o usan los virus con fines de lucro.

El presente informe intentará abarcar el tema anterior de una forma más detallada, comentando las definiciones de virus, Antivirus, Firewalls, Hackers y Crakers con sus definiciones y diferencias, el mercado de software Antivirus y sus códigos de ética, tanto para ingenieros como para vendedores de software. Trabajo tomado desde el punto de vista de personas con intenciones de informarse sobre el tema y poder informar a más personas de una manera más simple, abarcando todos los puntos que una persona a nivel de usuario debería saber, buscando información en la red de redes : Internet, tratando de buscar la coincidencia de los puntos de vista de ciertas páginas y revisar las diferencias en sus escritos, sacando la conclusión que, a nuestro pensar, es la que más se relaciona con el tema, alcanzando todos los puntos de vista posibles para llegar a un punto de vista común.

Esperando que el trabajo cumpla con los objetivos estipulados anteriormente damos paso a la tarea número 1 de Fundamentos de Programación, segundo semestre 2001, relacionado con virus, Antivirus y todo el tema que implica la batalla informática mundial.

La seguridad en los sistemas computacionales

Cuando debemos realizar algún trabajo utilizando medios computacionales siempre es necesario el software adecuado y este muchas veces posee elevados costos comparables incluso con los del hardware (si compramos programas originales) por lo tanto necesitamos tomar medidas de seguridad para conservar el software en buen estado y lejos de los ataques de virus y piratas informáticos. Esto visto desde el punto de vista personal pero para una empresa mayor esta seguridad es indispensable ya que mantener la integridad, confidencialidad y disponibilidad de los datos seria de vital importancia para una empresa que se apoya en un sistema computacional.

Los tipos de seguridad se dividen en física: contra daños materiales (descomposturas, fallas de energía, incendios, robo, etc.) y lógica: control de datos a fin de reducir el riesgo de transferencia, modificación, perdida o divulgación de los datos

La creación de un programa de seguridad deberá contener por lo menos las siguientes medidas:

Clasificación del personal, Sistema de control de acceso, Sistemas de protección de acceso de usuarios(password), Sistemas de protección de tiempo de espera en la terminal, Encriptación de archivos, Restricción del tiempo de acceso, Detección y expulsión de intrusos, Asignación de propiedades, Métodos de respaldo, Control de virus, Control de calidad del software, Monitoreo y auditoria de sistemas.

Para asegurar la permanencia de la información debe tener : Un disco de sistema, Por lo menos un programa Antivirus actualizado, Una fuente de información sobre virus informáticos, Un programa de respaldo de áreas criticas, Respaldos, Discos nuevos, Revisar a prestamos o prestados, Revisar todos los programas que obtengan por módem o redes, Revisar periódicamente la computadora.

Los temas más preocupantes en lo que respecta a seguridad son los relacionados con virus y piratas informáticos, temas que trataremos mas adelante con sus respectivas soluciones

¿Qué es un virus?

Un virus es un ente que ingresa al organismo y que se reproduce a si mismo para infectar a otras células del organismo, la misión del virus informático semejante, sólo que en este caso es un programa o código el cual ingresa a través de diversas vías a otros sistemas y se autoreproduce a si mismo creando varias copias y dañando, modificando e incluso eliminar la información en la memoria, casi la mayoría de las veces sin que el usuario se de cuenta hasta que sea demasiado tarde, cuando los archivos ya están borrados hasta que el computador quede inoperante por el ataque. Las características que se necesitan para que un virus sea virus son: que sea dañino, que se autoreproduzca y que sea subrepticio. Los virus

son generalmente el “juguete dañino” de cualquier programador que quiera probar sus habilidades y que al final lo único que logra es dañar a cientos de personas.

¿Cómo actúa un virus?

Un virus ingresa clandestinamente a los usuarios desde un sitio en internet, desde archivos infectados o en los bullettin boards (BBS), éstos al ingresar al sistema, comienzan a autoreproducirse, y cuando ya han infectado todos los archivos ejecutables (al infectar dejan una “marca” al archivo infectado para así no recontagiarlo) y luego comienzan a ejecutar su misión, o sea, dañar archivos, borrarlos, bloquearlos, además de imprimir mensajes sin sentido en la pantalla, también, en este instante el virus activa un sistema de defensa, en el cual trata de no ser detectado por algún Antivirus, y en otros casos se autodestruye para no dejar más rastro que los daños causados.

Elementos que generalmente se confunden con un virus.

Existen algunos programas que no son virus propiamente tales, pero que igual dañan al computador, entre éstos están los bug ware o fallas de software complejos que crean problemas después de ser usados por largo tiempo. Los caballos de troya, que por medio de engaños son ejecutados por el usuario causando diversos daños, los camaleones, que se hacen pasar por programas confiables para así atacar el sistema, las bombas, tanto lógicas, como de tiempo o software que dañan al computador con cierta fecha, clave o programa y los conejos, los cuales no destruyen datos sino que se autocopian hasta llenar el disco y saturar el sistema. Aunque los anteriormente no son virus propiamente tales, se les debe tener mucho cuidado.

Puntos propicios de infección de los virus informáticos

Los virus y los “no tan virus” atacan muchas partes del sistema de un computador, en las que se pueden destacar el sector de arranque o boot sector, lo cual provoca que en vez de cargarse la secuencia normal de booteo, se cargue primero el código del virus y luego lo demás, quedando el virus residente en memoria. Otro lugar estratégico para contaminar el sistema es el intérprete de comandos (Shell), aquí el virus contamina un solo archivo, pero pueden así interceptar todas las órdenes que el usuario le da al sistema y en algunas ocasiones engañar al usuario (ejemplo: mostrar un directorio y borrar todos los archivos del directorio, pero seguir mostrando el directorio, como si existieran archivos). También están los ataques a los archivos ejecutables para un propósito general, propagándose al ser ejecutado el archivo, éste es uno de los sistemas más usados, y muchas veces, para eliminar el virus, se deben eliminar los archivos. Y finalmente podemos mencionar a los residentes en memoria, que se instalan en memoria y allí permanecen hasta que el sistema se apague, pudiendo atacar en cualquier momento.

Algunos virus destacados

En esta parte vamos a describir a algunos virus que son importantes en este momento y que son “representativos” que son el Red Code (código rojo), el CPW y el CPW2 (los últimos dos chilenos).

A)Virus Código Rojo (Red Code) : En un virus tipo gusano, de procedencia desconocida, el cual tiene aterrado a todo el orbe computacional, especialmente a los usuarios de Windows 2000, NT y en el Internet Information Service que se usa como servidor de internet y que se aprovecha de un bug que Microsoft descubrió en los sistemas antes mencionados y, aunque ya se puso a disposición de los usuarios una "vacuna" hay muchos sistemas vulnerables por el momento. Este virus se propaga por internet causando demoras en el servicio y destruyendo páginas y durante los 20 primeros días de cada mes el virus se propaga por la red, aunque por el momento sólo ha dañado páginas en inglés (pero de todas maneras se debe estar muy atento) y se desconoce la amplitud del contagio. También se puede decir que este virus dejó en jaque a la Casa Blanca y al Pentágono.

B)Virus Chilenos: Para quien no lo crea nuestro país también tiene sus propios virus los cuales han dado que hablar en el país, en nuestra república hermana Argentina y otros países de habla hispana y son dos en especial, de los cuales daremos una pequeña reseña.

b.1)CPW y CPW2 (Chile Mediera) : Virus creados en La Serena, el primero aparecido en 1991, su ataque consiste en borrar archivos.EXE y .COM, además de borrar ciertos Antivirus, junto con imprimir en pantalla varias veces la frase : "Feliz cumpleaños CPW", "you are here CPW" (el primero) y "Viva Chile Mierda" (el segundo). En un principio eran confundidos con el "CB 1530" pero ahora pueden borrarse con cualquier Antivirus actualizado. Finalmente, estos virus poseen una falla, al tratar de borrar discos (tanto rígidos como diskettes) se queda leyendo indefinidamente.

Ejemplo de las consecuencias dejadas por un virus (en este caso es el virus Marburg)

Los Antivirus

Definición de Antivirus.

Un Antivirus es un programa que tiene como fin encontrar, clasificar y destruir cualquier organismo (llámese virus) que trate de ingresar al sistema del usuario, cosa que generalmente cuesta mucho, ya que, los virus van mutando a medida que van actuando, y aunque es una buena medida, no es 100% segura, por la gran velocidad con que se están creando los virus y sus diversas estructuras cada vez más complejas.

Tipos de Antivirus

Los Antivirus funcionan de acuerdo a diversos sistemas para detectar la presencia de un virus, entre los que se encuentra el sistema clásico o scanning, con el cual el Antivirus revisar el código de todos los archivos almacenados en la unidad (en especial los ejecutables), buscando trozos que pudiesen pertenecer a algún virus informático, método el cual se ha vuelto bastante ineficiente. Otro método es el de usar rutinas características de un virus y de acuerdo a esa base, encontrar posibles virus (un ejemplo son los algoritmos heurísticos), éste sistema es bastante más eficiente que el anterior, pero tiene la desventaja de que puede confundir a cualquier cosa y darla como virus (un caso del 1er tipo es el viruscan de Mc Afee y del segundo el conocido Norton Antivirus.)

Forma de operar de un Antivirus

Los Antivirus se conforman, por lo general de dos módulos, el primero, llamado módulo de control, es el que encarga de detectar e identificar el posible virus que ha ingresado, y algunos, en este módulo tienen un verificador de integridad que revisa el registro de cambio en archivos ejecutables y zonas críticas del disco rígido. El segundo módulo es el módulo de respuesta, en el cual, el Antivirus alerta al usuario, cuando sospecha de un virus y, en algunos casos, dar la opción de eliminar el posible virus.

Piratas informáticos

Otro de los grandes peligros que existentes en la actualidad son la presencia de los Piratas informáticos más conocidos como hackers y crackers, este problema es mucho mayor que el que representan los virus, ya que estos son personas con un alto grande de conocimiento en el campo de la informática, estos pueden usar sus conocimientos tanto para el bien (gracias a su experiencia pueden crear sistemas de seguridad menos vulnerables) como para el mal (crear virus, robar contraseñas, destruir sistemas,etc.).

Nótese que los Hackers no son criminales . En el mejor de los casos, son los incentivadores, probadores y aprobadores de las mejores y más nuevas tecnologías. En el peor, los Hackers pueden ser traviesos, perversos y delincuentes curiosos. Entre los Hackers existen niveles sociales y de ahí nacen los ELEET (elite), que son los que más saben sobre su trabajo y los LAMER (lammer) que son los que juran ser Hackers, que procuran conocer y arrimarse a uno, aunque nunca hayan hecho nada notable.

Etica de Hacker

Desde hace tiempo circula por Internet el auto denominado Código de Etica de los Hackers, que trata de mantener claras sus motivaciones, objetivos y por sobre todo, que trata de mantener alejados a los controladores de la ley.

1_El acceso a las computadoras y a cualquier cosa que pueda enseñarte algo acerca de la forma en que funciona el mundo debe ser total e ilimitado. 2_Apelar siempre a la imperativa: ¡Manos a la obra! 3_Toda información debe ser libre y/o gratuita. 4_Hay que desconfiar de la autoridad. Hay que promover la descentralización. 5_Los Hackers deberán ser juzgados por sus hackeos, no por falsos criterios como títulos, edad, raza, o posición. 6_En una computadora se puede crear arte y belleza. 7_Las computadoras pueden cambiar la vida para mejor.

Por otro lado un hacker con sed de ego, espíritu destructivo, necesidad económica o que esta recién empezando y no toma conciencia de los daños que puede ocasionar puede llegar a convertirse en un cracker y realizar actividades dañinas en contra de algún sistema computacional. Un Cracker puede ser un niño travieso, un joven delincuente o un gran profesional contratado por una gran corporación. Lo que sí, no podemos evitar aceptar que están presentes por cintos en el Internet y que en general, están buscando problemas.

Los delitos que puede llegar a cometer un pirata informático son variados. El término "pirata" se aplica en sentido amplio a todo quién hace algo indebido con recursos de programación. Pero se han de distinguir diferentes conceptos y realidades más precisos:

En términos estrictos, el "pirateo" designa la reproducción (copia) ilegal de aplicaciones. Esta es un atropello a los derechos intelectuales del creador del software y a los derechos económicos de quienes financiaron su producción. Las grandes compañías de software pierden millones de dólares por concepto de "pirateo", lo cual encarece el costo de las copias legítimas que podemos adquirir en los negocios del ramo. En este sentido, toda persona que realiza una copia ilegal comete un delito (y es un "pirata").

Una persona que posee mas conocimientos puede realizar acciones mas elaboradas y peligrosas como lo son el acceso a informaciones confidenciales y la destrucción de datos o de software.

Dado la globalización de los recursos computacionales estos piratas informáticos son cada vez más peligrosos ya que en la actualidad poseen avanzadas herramientas de crackeo y en muchos de los casos son estos los principales creadores de virus que no poseen otro fin que el de destruir.

Algunos delitos en redes computacionales reconocidos:

Virus: Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos o por la Red. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos: Se fabrica de forma análoga al virus con miras a infiltrarlo en alguna red o en programas legítimos de procesamiento de datos o para modificar o destruir los datos en una red, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba lógica o Cronológica: Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Reproducción no autorizada de programas informáticos de protección legal: Esta 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 problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Address Spoofing En el caso de redes conectadas a Internet, los hackers pueden alterar su identidad, haciendo creer al computador que da acceso a una determinada institución que son computadores "autorizados" a ingresar o confiables (Address Spoofing). Existen numerosos procedimientos, pero describirlos más ampliamente va más allá de objetivo del presente informe.

Caballos de Troya Se instalan en una estación del sistema un pequeño programa que captura la secuencia de teclas digitadas, y actúa solapadamente capturando y guardando en un archivo todo lo que se digita después de ciertas palabras clave (como "login", "username", "nombre" o "password" por ejemplo). Posteriormente, el hacker revisa desde un lugar remoto el contenido del archivo que obtuvo. Esta técnica es relativamente simple, y generalmente nadie nota nada.

Firewalls

Dado lo peligrosamente vulnerables que se han vuelto actualmente las redes es necesario contar con alguna barrera que controle el flujo de información y evite así la entrada de intrusos al sistema, esta es la tarea de la cual se encargan los firewalls los cuales son una importante herramienta de seguridad en la actualidad.

Los firewalls tienen como principal función: impedir accesos a usuarios no autorizados (no importa si viene de red local o internet) , bloquear algunos programas troyanos y otras aplicaciones capaces de dañar el sistema y examinar el contenido de la información que se esta obteniendo para determinar si se le permite el paso a nuestra computadora o no (filtrado). Las políticas de control de los datos que ocupa varia de acuerdo al firewall que se utilice. Hay tres tipos de firewalls: 1 filtran los datos en base a sus contenidos y dirección IP 2 solo permiten la comunicación entre computadoras admitidas y proveedores de servicio de internet 3 que realiza una inspección de estado controlando la configuración de los paquetes para decir si son útiles o no y luego decide si bloquea o no el paso de la información. Para que un firewall sea efectivo, todo trafico de información a través de internet deberá pasar a través del mismo para ser inspeccionado

Los firewalls se diferencian también por su complejidad, así, una empresa que posea una gran cantidad de información confidencial o un gran capital en software requerirá de un firewall mucho más eficaz pero que necesitara de una mantención constante, ya que un firewall no es 100 % seguro, siempre posee una pequeña falla que encontrara algún hacker y deberá ser reparada, ya que los firewalls reciben la información y deciden si esta pasa o no, pero la información ya se recibió.

Un buen ejemplo del funcionamiento del firewall es aquel que compara el puerto que protege el firewall con un tubo, El firewall tapa uno de los extremos del tubo, luego analiza la información, si la información cumple con los requisitos impuestos por el firewall, pasa a las aplicaciones del computador sino llega hasta ahí no más.

Cuando los paquetes llegan al computador, van al OTRO extremo del tubo - el extremo TCP/IP. Si el propósito del paquete es dañar el extremo que lo recibe, es inútil cerrar el puerto hacia la aplicación. Más aun, es imposible protegerse contra todos los tipos de ataque, lo que demuestra que no es 100% efectivo.

Entonces podemos considerar a los firewalls como un buen sistema de seguridad, pero no debe dejarse todo en sus manos, sino que debe implementarse con Antivirus

Legislación jurídica de delitos informáticos

. En el último tiempo, tanto en nuestro país como en el mundo la informática se ha convertido en un arma de doble filo para todos, ya que, puede ayudarnos a realizar muchas cosas y al mismo tiempo, puede dejar información confidencial al alcance de personas inescrupulosas y con malos propósitos que son capaces de ocasionar grandes disturbios con sus acciones, es por ese motivo que muchos países han tomado medidas en sus legislaciones contra los delitos informáticos (para crímenes como narcotráfico, destrucción de información, estafas, terrorismo, etc.)

Resumen sobre los tipos de delitos

Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.

Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.

Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.

Interceptación de e-mail: : Lectura de un mensaje electrónico ajeno.

Estafas electrónicas: A través de compras realizadas haciendo uso de la red.

Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.

Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

De acuerdo con la Organización de las Naciones Unidas (ONU), la falta de acuerdos globales sobre la definición legal de las conductas delictivas electrónicas, la ausencia de leyes procesales y tratados de extradición y ayuda mutua que permitan vigilar la red, son las causas para que Internet se haya convertido en un foco de criminalidad.

Sobre Legislación internacional cabe decir que son pocos los países que tiene legislación contra delitos informáticos (al menos una eficiente) entre los que están Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España y Chile

Chile fue el primer país de Latinoamericano en sancionar una ley contra delitos informáticos, la que entró en vigencia el 7 de Junio de 1993. Según ella, la destrucción o inutilización de datos de un ordenador es sancionado con prisión que va desde un año y medio hasta 5 años, incluyéndose dentro de este tema los virus. Esta ley muestra en el artículo 1 el tipo legal vigente de una personan que quiere destruir o inutilizar los datos de un sistema de información e impida su correcto funcionamiento y el artículo 3 tipifica la conducta maliciosa que provoca daños o alteraciones en un sistema de información, siendo en otros países mucho más rígida y severa, como es el caso de Estados Unidos, donde inclusive hay una brigada informática especialmente diseñada para estos y detallada sobre el tema.

Código de ética y Práctica Profesional en el Diseño de Software

Debido a la gran variedad de acciones que puede realizar un Ingeniero en Software, tanto malas como buenas con sus proyectos, el siguiente código pretende guiar al Ingeniero a que realice un bien antes que un mal con sus trabajos.

El Código contiene ocho principios referidos al actuar de los Ingenieros de Software profesionales, estos principios están mirados desde el enfoque ético y responsable que deben tener los ingenieros al momento del desarrollo de un software.

Estos principios tienen su base en la humanidad del Ingeniero y en la gente que es afectada por el trabajo de este.

El Código no solo juzga actos cuestionables sino que además cumple una función educativa.

Conforme al compromiso de salud, seguridad y bienestar del público los Ingenieros en Software se adherirán a los siguientes ocho principios.

1._ EL PÚBLICO:

Los Ingenieros en Software actuarán coherentemente con el interés del público de acuerdo a los siguientes puntos.

Aceptar la responsabilidad de su trabajo, Aprobar el Software sólo si ellos tienen una creencia fundada que esto es sano y salvo, Revelar cualquier peligro del software, real o potencial, al usuario, el público o el ambiente, Evitar el engaño en todas las declaraciones acerca del Software.

2._ CLIENTE PATRÓN

Los Ingenieros de Software actuarán en una manera que está en los intereses de

de su cliente y patrón, compatible con el interés del público de acuerdo a los siguientes puntos :

Usar la característica de un cliente o patrón debidamente autorizada, Mantener en privado cualquier información ganada por medio de su trabajo._ Informar al Cliente o Patrón si un proyecto va a fallar, violara la ley de propiedad intelectual o si no será problemático, No aceptar ningún trabajo exterior perjudicial al trabajo que ellos realizan para su patrón primario, No promover ningún interés adverso a su patrón o cliente, a no ser que una preocupación ética sea comprometida.

3._ PRODUCTO

Los Ingenieros de Software asegurarán que sus productos se encuentran en las normas profesionales más altas, en particular:

Esforzarse por la alta calidad del producto, Asegurar objetivos apropiados y viables para cualquier proyecto, Definir las cuestiones éticas, económicas, culturales, legales y ambientales para trabajar proyectos, Asegurar que los datos específicos para el software sobre el que ellos trabajan han sido documentados, y satisfacen las exigencias de los usuarios.

4._ JUICIO

Los ingenieros de software mantendrán la integridad y la independencia en su juicio apropiado.

Atenuará los juicios técnicos por la necesidad de apoyar y mantener valores humanos, Sólo aprobará documentos con los que él esté de acuerdo, Mantendrá la objetividad profesional relacionados con software o documentos que se le pide aprobar, No cometerá prácticas impropias financieras.

5._ DIRECCIÓN

Los gerentes y líderes del software promoverán un desarrollo ético a la dirección de desarrollo de software y a su mantenimiento.

Dirigirá por buen camino cualquier proyecto sobre el que ellos trabajen, Asegurar que los Ingenieros de Software saben la política del patrón y los procedimientos para la protección de contraseñas, archivos y información que es confidencial al patrón, No pedir a un Ingeniero de Software hacer algo en contra de este código.

6._ PROFESIÓN

Los Ingenieros de Software elevarán la integridad y la reputación de la profesión compatible con el interés del público.

Promover el conocimiento público de Ingeniería de Software, Apoyar a otros Ingenieros que se esfuerzan por seguir este código, No promover el interés propio a cargo de la profesión, el cliente o el patrón, Obedecer todas las leyes que gobiernen su trabajo, Evitar conexiones con negocios que están en conflicto con este código

7._ COLEGAS

Los ingenieros proporcionarán apoyo a sus colegas.

Promoverá a sus colegas a seguir este código, Ayudara a colegas en el desarrollo de software, Dar vista imparcial a las opiniones, preocupaciones o quejas de sus colegas, En situaciones fuera de sus propias áreas de capacidad, apelará a opiniones de otros profesionales.

8._ MI

Los ingenieros de Software participaran en un estudio de toda la vida en cuanto a la práctica de su profesión y promoverán un acercamiento ético a la práctica de la profesión.

Mejorará su capacidad de crear la caja fuerte, el software de calidad y útil con un costo razonable y en tiempo razonable, Mejorará su capacidad de producir una documentación exacta y bien escrita, Mejorar su conocimiento del software y documentos relacionados sobre los que ellos trabajan y del ambiente en el que ellos serán usados, Mejorar su conocimiento de este código, Reconocer que las violaciones personales a este código son incoherentes con ser un Ingeniero de Software Profesional.

Aplicaciones

Políticas de seguridad para el sistema computacional del DIINF (Depto. Ingeniería en Informática).

El DIINF es un lugar en la que una gran cantidad de personas trabaja usando un mismo sistema y no sería difícil que un virus atacara el sistema y terminará dejando paralizado de departamento durante un buen tiempo, como aplicación a lo anterior se intentarán dar algunas medidas que podrían (si es que no están ya) ser usadas en el DIINF.

1.-Tener un buen sistema Antivirus, y si se puede, tener dos funcionando a la vez (sin que se topen entre ellos), ya que, las probabilidades de detectar y eliminar al virus son mayores, (ojalá que el Antivirus sea actualizado antes de tres meses). Además de tener una fuente de información sobre virus (llámese programa, libro, archivo de texto), que contenga síntomas, descripción y características de los 100 virus más conocidos por lo menos. Y además tener un Firewall lo suficientemente eficiente y con actualizaciones y revisiones periódicas para que la información que ingrese al sistema sea “filtrada” por él, y al mismo tiempo prevenir el ingreso de Hackers y Crackers(especialmente los segundos) al sistema

2.-Tener programas de respaldo para zonas críticas, o sea backups de sectores de arranque, tanto de diskettes como de discos rígidos, además de tener un disco de sistema protegido contra escritura (para que pueda ser arrancado desde allí en caso de problemas), revisar los programas que se ingresan (en especial los que son ingresados al computador central), además de revisar periódicamente la computadora, para cerciorarse de que el sistema este en excelente condiciones, junto con la cooperación de todas las personas que trabajan en el departamento, para así, poder evitar la inserción de algún virus en los equipos.

Normas para proteger nuestros computadores en casa.

En el hogar es más fácil que ocurra una infección de virus el computador, ya que, muchos juegos suelen ser bajados por internet, además de demos de juegos, programas compactadores, de interés para los integrantes de la familia, etc, por lo que daremos unas ayudas que pueden ser muy útiles al momento de presentarse un virus en nuestro hogar.

.

1.- Tener un buen programa Antivirus, en lo posible, actualizado cada tres meses (según nos informamos, probablemente exista en el mercado un firewall casero, ya que, los normales son bastante caros, y estos son muy buenos contra hackers y crackers), tener información de por lo menos los 100 virus más conocidos, con sus posibles formas de atacar y sus curas, revisar todos los discos que han sido prestados, además de revisar los discos nuevos antes de usarlos (más vale prevenir que curar), revisar todos los programas que se bajen por módem o redes, tener respaldos de programas importantes, de zonas críticas, una lista de lugares donde acudir en caso de fallas por virus, además de un programa de protección residente (generalmente los Antivirus traen uno) y un disco de sistema protegido contra escritura y libre de virus, que contenga por los menos los siguientes comandos: FORMAT, FDISK, MEM y CHKDSK (o SCANDISK en versiones recientes de MS-DOS).

Tanto e nuestra casa como en el trabajo, en este caso el departamento, es preferible tomar ciertas medidas, como las anteriores para así estar medianamente seguros del ataque de virus, hackers, crackers y cualquier enemigo cuya intención sea robarnos información o acabar con nuestro computador por simple diversión.

Opiniones sobre aspectos controversiales sobre el tema.

Sobre las fuentes de información para el trabajo, se debe decir que hablaban sobre el tema de una manera clara y precisa, en especial el de monografías.com y softdownload.com, pero lo problemático no es que las fuentes den buena información, ya que, aún hay gente desinformada que confunde el accionar de un hacker con el de un cracker, viéndose que tanto sus fines como su accionar son diferentes, ya que, los primeros son "ayudas" para mejorar los sistemas de seguridad, mientras los segundos sólo tratan de hacer daño. Otro punto controversial es que las empresas deberían ser más transparentes en sus acciones, ya que, como se vio anteriormente, se han dado casos de que empresas de software Antivirus, crean virus para así vender sus productos. Es hora de que la gente tome conciencia y diga basta a este juego de nunca acabar, en el cual los únicos perjudicados son los usuarios.

Resumen

En una sociedad corporativa, a diferencia de un hogar, los sistemas computacionales y el software que manejan deben ser protegidos todo el tiempo de los peligros, tanto físicos como de información, peligros como los hackers, que son personas con conocimientos sobre el tema computacional y tratan de encontrar el punto débil de grandes corporaciones o páginas web para así, en parte demostrar su habilidad. Los crackers son similares en rasgos que los hackers, sólo que éstos últimos ingresan a información ajena con el fin de destruirla y de causar un sinnúmero de molestias que a veces llegan a costarle millones de dólares a los afectados. Un medio por el cual no sólo los hackers y cracker, sino que cualquier persona con conocimientos, puede dañar a otros usuarios es por medio de virus (llámese como virus a todas sus variantes, incluidos los no virus propiamente tales, como troyanos, camaleones, conejos, etc.), cuyo fin es, entre varias, autoreproducirse, infectar activos causando la alteración o destrucción de éstos, llegando a veces a dejar inoperante el sistema, llegando al usuario por medio de engaños o directamente al ejecutar archivos o ver páginas web. Atrapar y destruir a éstos "organismos" no es cosa fácil, pero existen

herramientas que nos simplifican el trabajo, como son los Antivirus y los Firewalls, los primeros, más al alcance de las personas, usando diversos métodos, detectan al intruso y muchas veces dan la opción de erradicarlo, pero que debe ser actualizado cada pocos meses, lo cual ha llevado a problemas, porque se han dado controversias de que los mismos creadores de Antivirus, están fabricando virus para continuar vendiendo sus productos. Los segundos, son muy elevados en costo, ya que requieren una preparación más específica y su utilidad es más alta, ya que, evitan que pase información peligrosa a la red y a la vez, evitan que intrusos, como hackers y crackers ingresen a nuestro sistema a quitarnos información, y aunque requieren actualización, no debe ser tan constante (a veces) como con los Antivirus, por lo general necesita ser reacondicionado para que sea más exigente con su protección. Aunque, también depende de la mentalidad de las personas que aprenden métodos de programación y control de estos sistemas, ya que, existen códigos de ética que siempre alguien con criterio los respeta, y si no, se enfrentará con la legislación vigente contra delitos informáticos que, aunque no es muy estricta, ha ido perfeccionádose a través del tiempo en muchos países del orbe.

Conclusión

Al concluir el trabajo, analizando información encontrada en la red de redes, Internet, se intentó mostrar de manera sencilla y rápida definiciones de virus, Anrtivirus y todo lo que se relaciona con el tema de sistemas informáticos, viendo que muchas páginas tenían opiniones diversas sobre el tema, las cuales hubo que organizar y buscar sus puntos de concordancia para poder elaborar un informe relativamente completo para que la persona que lo lea, logre captar la idea de lo que ocurre con los programadores destructivos y lo dañinos que pueden ser si no se toman las medidas necesarias. Por eso el fin de mostrar las características de un virus, de un Hacker y de un Cracker (para poder reconocerlos), y las de un Antivirus y un firewall, para que se pueda escoger el más adecuado y no caigamos en una estafa, además de aplicar los conocimientos adquiridos en la elaboración de algunas formas de mejorar el sistema de prevención de la red del DIINF y de la casa de cualquiera de nosotros para que así no caigamos tan fácilmente en este problema, ya que, aunque existen medidas a tomar, éstas no son 100% seguras y constantemente deberemos estar atentos ante una posible amenaza de virus o de pérdida de información.

El trabajo se vio desde el punto de vista de un usuario simple que comenzó a estudiar de poco la información (y que de paso tuvo que eliminar ciertos virus) y que analizando información de diversas fuentes, se buscó la mejor forma de enfrentar el problema.

Obviamente, al concluir el trabajo, logramos llegar a los objetivos esperados, sin dejar de decir que este trabajo no queda aquí, ya que depende de cada uno seguir actualizándose en el tema(así como un Antivirus), ya que, por el momento este es un tema de nunca acabar, porque virus tenemos para mucho tiempo mientras a alguien (o entre todos) se le ocurra una solución al 100%, mientras, deberemos estar a la defensiva.

Bibliografía

http://www.khainata.com/extrainternet/hackers.html

http://www.puc.cl/curso_dist/cbc/anexos/texto_a/piratas.html

http://bbs.seker.es/~alvy/Hacker-Cracker.html}

http://www.cyberangels.com/international/espanol/net-ed/firewalls.html

http://www.softdownload.com.ar/firewallnota.htm