UNIVERSIDAD DEL VALLE DE MÉXICO

CAMPUS SAN RAFAEL

ALMA MATER

El VIRUS, INFECCIÓN CIBERNÉTICA

MÉXICO DF 2001

INDICE

TEMA PAGINA

I. INTRODUCCIÓN

No existe hoy en día una política antivirus que sea 100% efectiva. La forma de evitar desastres es mantenerse al tanto de las últimas novedades en seguridad informática existentes en el mercado en la forma de paquetes antivirus, sumando una buena gestión del sistema de discos. También es importante mantenerse al tanto de algunos métodos caseros de identificar y erradicar infecciones de virus descubiertas recientemente y que con seguridad no están incluidas en la lista de virus conocidos que su antivirus detecta.

La consigna principal es tener un buen programa antivirus instalado en el sistema y mantenerse al tanto de las actualizaciones que tiene dicho producto.

Un programa antivirus por muy bueno que sea se vuelve obsoleto muy rápidamente ante los nuevos virus que aparecen día con día.

Por otro lado, los administradores de red deben tomar precauciones y establecer políticas a fin de prevenir la introducción de virus, así como identificar y erradicar los que llegaran a introducirse. Toda red debe poseer un software especial que contribuya a mantener una red libre de virus.

Existen sistemas de prevención que intentarán parar el virus en el mismo momento en que se produzca el ataque. Un buen método es impidiendo el acceso al sistema a programas o usuarios que no tengan autorización. El sistema de detección comprueba el código del programa antes de que se ejecute. El usuario podrá ser avisado de los posibles peligros del programa que va a ejecutarse. No es que los sistemas de detección sean más cómodos para el usuario. Realmente hoy en día muchos de los antivirus del mercado juntan ambos sistemas en mayor o menor medida.

La creación de nuevos virus es un problema creciente, como sus homólogos biológicos, dado el crecimiento exponencial parecido al de una colonia de bacterias sin enemigos naturales, los virus no tienen otro enemigo que no sean los programas antivirus; los virus se producen en una cantidad exorbitante. Los programas antivirus crecen con una curva mucho más suavizada, es decir, lo que se observa es que los diferentes programas de antivirus se van quedando rezagados con respecto a los virus informáticos.

Esto afecta de manera importante a un establecimiento de Café Internet, ubicado en calle Tixtla # 39 Col. Sn Felipe de Jesus, ya que está expuesto todo el día a los virus, por lo tanto, es necesario encontrar una forma de

detener a estos programas destructores, evaluando a conciencia las tecnologías que en la actualidad nos ofrecen

Este planteamiento me llevaría a elaborar los siguientes cuestionamientos:

- Mediante un programa de software ¿se podrá ampliar la protección contra los virus en Internet?
- Por medio de advertencias sobre los virus formuladas en carteles y colocadas frente a cada computadora en un Café Internet se disminuiría el contagio de virus
- Específicamente en un Café Internet ¿se podría prevenir la infección de virus mediante la instalación de sistemas de protección para red?

Es importante conocer los daños que causan los virus a la información que se encuentra en nuestras computadoras, y aprender a evitar su contaminación, ya que no sólo dañan archivos, sino también puede llegar a afectar al disco duro ocasionando problemas irreversibles.

En el Café Internet se descompusieron siete maquinas, debido a que un usuario, al no estar enterado del último virus que se había creado, descargó de Internet un archivo infectado, dañando así varias maquinas, ya que se encuentran en Red. El Virus pasó de una computadora a otra, introduciéndose a los archivos del sistema, afortunadamente no se ocasionó un daño irreversible.

Por consecuencia tuvieron que mandar a arreglar las computadoras, se tardaron quince días en entregárselas. Debido a este problema, el Café Internet tuvo problemas económicos.

Con esta investigación se darán a conocer los tipos de virus más frecuentes, los más peligrosos, métodos de prevención y corrección, tipos de sistemas y cuáles son más efectivos y si el mal ya esta hecho cómo remediarlo.

Por lo tanto los objetivos de este trabajo son los siguientes:

- Analizar la información de lo que son los Virus.
- Evaluar los sistemas de protección que existen para la Red en un Café Internet.
- Comparar los diferentes Antivirus que están en el mercado, y proponer el mejor para implantarlo en el Café Internet

II. MARCO TEÓRICO

Los virus pueden dañar seriamente la computadora, por eso es importante realizar una copia de seguridad de todos los archivos importantes que se guardan en el disco duro y tenerlos en un lugar seguro.

También hay que actualizar los antivirus, las actualizaciones muchas veces se pueden bajar de la Internet o se pueden comprar.

Es muy importante tener un antivirus actualizado ya que cada día se crean mas y más virus que pueden ser mortales para nuestra computadora.

Cómo solucionar los problemas de corrupción de datos por virus. Existen virus que pueden dañar su sistema a causa de la transferencia de archivos contaminados.

Cuando baje un archivo, es esencial que utilice un detector de virus a fin de evitar todas las formas de contaminación que pueden dañarlos datos de su disco duro. En efecto, varios piratas de la computación tienen como pasatiempo insertar en el software los virus que en ocasiones se convierten en verdaderas bombas de efecto retardado. El único objetivo de este virus es ocasionar problemas de funcionamiento en su

computadora.

Para evitar los dolores de cabeza y la paranoia que produce este problema potencial, lo ideal es utilizar un programa detector de virus.

Hay que comprobar que el manejo y la rapidez del antivirus son lo bastante como para que usted no le desagrade realizar un barrido completo del disco duro por lo menos una vez a la semana.

También tiene que comprobar que cuando se ejecute el antivirus sea exclusivamente el solo y no permitir que otros programas se ejecuten.

Los virus son muy peligrosos estando en Internet ya que hay demasiados usuarios ya sea revisando su correo, bajando archivos, consultando paginas, etc. ase poco tiempo había un virus que se llamo Love este se encontraba en el correo electrónico llegaba un mensaje con ese nombre y cuando lo habrías para ver que contenía se ejecutaba el virus y se regaba por todo el sistema

Internet se podría definir como una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios. A Internet están conectados artistas, funcionarios, académicos, burócratas, investigadores, gente de negocios, estudiantes, etc.

Los virus se fabrican a veces por causas políticas, y principalmente como diría un psicólogo, por dementes entendiendo por demente en este caso a una persona que hace esto para intentar realizarse, por lo regular son tipos inmaduros y no tienen mayor motivación que arruinarla la información a los demás y dañar la maquinas, claro menos la de ellos.

Internet se podría definir como una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios. A Internet están conectados artistas, funcionarios, académicos, burócratas, investigadores, gente de negocios, estudiantes, etc. Internet es simplemente una red de redes donde cada red o incluso cada ordenados, es una isla gobernada de forma local. Internet basa su utilidad básicamente en cuatro servicios: correo electrónico, servicio de noticias, acceso remoto y transferencia de ficheros.

Un virus es ante todo un código informática capaz de reproducirse así mismo y atacar a un programa inofensivo sin conocimiento del usuario, con intenciones malignas y destructivas. Recuerde que el **Caballo de Troya** se hará pasar por inofensivo aunque producirá daños en el ordenador en el que se introduzca.

Tenga bien en cuenta esto. Un virus es maligno. Olvídese de esas fábulas de los virus simpáticos. **No existen**

El virus se aprovecha de la ignorancia. Un usuario medio tiene grandes dificultades en detectar un virus por falta de conocimientos.

Es totalmente normal que el usuario del montón se sienta un poco desvalido e intimidado por su ordenador. Siempre se puede producir algún problema repentino, cadenas sueltas, programas degradados por él pirateo. En su mayoría no ofrecen demasiados problemas y se resuelven fácilmente con unos pequeños trucos. Pero un usuario normalmente no los conoce por lo que realmente no puede distinguir entre un problemita y un VIRUS.

Un virus trata de hacer el mayor daño posible y como una vez descubierto es demasiado vulnerable utilizara toda clase de trucos para mantenerse en secreto el mayor tiempo posible. Cuando un virus es descubierto, invariablemente se detecta todo un rastro de ordenadores infectados.

III. MÉTODO

El método que se utilizará es de metodología de investigación en donde: para recopilar la información se utilizo la investigación científica y la de campo. En la investigación científica se consultarán libros, Internet, Revistas, etcétera.

Para la investigación de campo se realizarán cuestionarios para determinar si los usuarios tiene el conocimiento de lo que son los virus y si están consientes del peligro que representan.

IV. CONTENIDO DEL TRABAJO

4.1. Análisis de lo que son los virus

4.1.1 Definición de Virus

Un virus es una pieza de software diseñada y escrita para afectar adversamente su computadora, alterando la forma en que trabaja sin su permiso o conocimiento.

En términos más técnicos, un virus es un segmento de código de programación que se implanta a sí mismo en un archivo ejecutable y se multiplica sistemáticamente de un archivo a otro.

Los virus de computación no se generan espontáneamente: Deben ser escritos y tener un propósito específico.

Usualmente un virus tiene dos funciones distintivas:

- Se reproduce a sí mismo de un archivo a otro sin su intervención o su conocimiento.
- Implementa el síntoma o daño planeado por el perpetrador.

Eso podría incluir borrar un disco, corromper sus programas o simplemente crear un caos en su computadora. Técnicamente, esto es conocido como el "cargamento" del virus, que puede ser benigno o maligno a voluntad del creador del virus.

Un virus benigno es uno que no está diseñado para causar un daño real a su computadora.

Por ejemplo, un virus que se esconde hasta un momento o fecha predeterminado y entonces lo único que hace es mostrar algún tipo de mensaje, es considerado benigno.

Un virus maligno intenta infligir un daño malicioso a su computadora, aún cuando el daño pueda no ser intencional. Hay un número significativo de virus que causan daños reales debido a mala programación y auténticos defectos en el código viral.

Un virus maligno podría alterar uno o más de sus programas de modo que no trabaje como debiera. El programa infectado podría terminar anormalmente, escribiendo información incorrecta en sus documentos.

O el virus podría alterar la información sobre los directorios en una de sus áreas de sistema. Esto podría impedir que la partición sea montada, o que Ud. no pudiese correr uno o más programas, o que los programas no pudieran localizar los documentos que Ud. quiere abrir.

Algunos de los virus identificados son benignos; sin embargo, un alto porcentaje de ellos son muy malignos. Algunos de los virus más malignos borrarían todo su disco duro, o borrarían archivos.

4.1.2 Clasificación

- Virus de Macros / Código Fuente. Se adjuntan a los programas Fuente de los usuarios y, a las macros

utilizadas por: Procesadores de Palabras (Word, Works, WordPerfect), Hojas de Cálculo (Excell, Quattro, Lotus).

- Virus Mutantes. Son los que al infectar realizan modificaciones a su código, para evitar ser detectados o eliminados (NATAS o SATÁN, Miguel Ángel, por mencionar algunos).

- Gusanos. Son programas que se reproducen a sí mismos y no requieren de un anfitrión, pues se "arrastran" por todo el sistema sin necesidad de un programa que los transporte.

Los gusanos se cargan en la memoria y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borrados los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdida de datos.

- Caballos de Troya. Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de algún tiempo, y esperando la indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones.

- Bombas de Tiempo. Son los programas ocultos en la memoria del sistema o en los discos, o en los archivos de programas ejecutables con tipo COM o EXE. En espera de una fecha o una hora determinadas para "explotar". Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al llegar el momento de la "explosión". Llegado el momento, se activan cuando se ejecuta el programa que las contiene.

- Auto replicables. Son los virus que realizan las funciones mas parecidas a los virus biológicos, ya que sé autor reproducen e infectan los programas ejecutables que se encuentran en el disco. Se activan en una fecha u hora programadas o cada determinado tiempo, contado a partir de su última ejecución, o simplemente al "sentir" que se les trata de detectar. Un ejemplo de estos es el virus del viernes 13, que se ejecuta en esa fecha y se borra (junto con los programas infectados), evitando así ser detectado.

- Infectores del área de carga inicial. Infectan los diskettes o el disco duro, alojándose inmediatamente en el área de carga. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo.

- Infectores del sistema. Se introducen en los programas del sistema, por ejemplo COMMAND.COM y otros que se alojan como residentes en memoria. Los comandos del Sistema Operativo, como COPY, DIR o DEL, son programas que se introducen en la memoria al cargar el Sistema Operativo y es así como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver sus carpetas (también llamadas: folders, subdirectorios, directorios).

- Infectores de programas ejecutables. Estos son los virus más peligrosos, porque se diseminan fácilmente hacia cualquier programa (como hojas de cálculo, juegos, procesadores de palabras).

4.1.3 Historia de los Virus Informáticos

Los virus tienen la misma edad que las computadoras. Ya en 1949 John Von Neumann, describió programas que se reproducen a sí mismos en su libro "Teoría y Organización de Autómatas Complicados". Es hasta mucho después que se les comienza a llamar como virus. La característica de auto−reproducción y mutación de estos programas, que las hace parecidas a las de los virus biológicos, parece ser el origen del nombre con que hoy los conocemos.

Antes de la explosión de la micro computación se decía muy poco de ellos. Por un lado, la computación era secreto de unos pocos. Por otro lado, las entidades gubernamentales, científicas o militares, que vieron sus equipos atacadas por virus, se quedaron muy calladas, para no demostrar la debilidad de sus sistemas de seguridad, que costaron millones, al bolsillo de los contribuyentes. La empresa privadas como Bancos, o grandes corporaciones, tampoco podían decir nada, para no perder la confianza de sus clientes o accionistas. Lo que se sabe de los virus desde 1949 hasta 1989, es muy poco.

Se reconoce como antecedente de los virus actuales, un juego creado por programadores de la empresa AT&T (mamá Bey), que desarrollaron la primera versión del sistema operativo Unix, en los años 60. Para entretenerse, y como parte de sus investigaciones, desarrollaron un juego, "Core War", que tenía la capacidad de reproducirse cada vez que se ejecutaba. Este programa tenía instrucciones destinadas a destruir la memoria del rival o impedir su correcto funcionamiento.

Al mismo tiempo, desarrollaron un programa llamado "Reeper", que destruía las reproducciones hechas por Core Ware. Un antivirus o antibiótico, al decir actual. Conscientes de lo peligroso del juego, decidieron mantenerlo en secreto, y no hablar más del tema. No se sabe si esta decisión fue por iniciativa propia, o por órdenes superiores.

En 1982, los equipos Apple II comienzan a verse afectados por un virus llamado "Cloner" que presentaba un mensaje en forma de poema.
El año siguiente, 1983, el Dr. Ken Thomson, uno de los programadores de AT&T, que trabajó en la creación de "Core War", rompe el silencio acordado, y da a conocer la existencia del programa, con detalles de su estructura, en una alocución ante la Asociación de Computación.

La Revista Scientific American a comienzos de 1984, publica la información completa sobre esos programas, con guías para la creación de virus. Es el punto de partida de la vida pública de estos aterrantes programas, y naturalmente de su difusión sin control, en las computadoras personales. Por esa misma fecha, 1984, el Dr. Fred Cohen hace una demostración en la Universidad de California, presentando un virus informático residente en una PC. Al Dr. Cohen se le conoce hoy día, como "el padre de los virus". Paralelamente aparece en muchas PCs un virus, con un nombre similar a Core War, escrito en Small−C por un tal Kevin Bjorke, que luego lo cede a dominio público. ¡La cosa comienza a ponerse caliente!

El primer virus destructor y dañino plenamente identificado que infecta muchas PC's aparece en 1986. Fue creado en la ciudad de Lahore, Paquistán, y se le conoce con el nombre de BRAIN. Sus autores vendían copias pirateadas de programas comerciales como Lotus, Supercalc o Wordstar, por suma bajísimas.

Los turistas que visitaban Pakistán, compraban esas copias y las llevaban de vuelta a los EE.UU. Las copias pirateadas llevaban un virus. Fue así, como infectaron mas de 20,000 computadoras. Los códigos del virus Brain fueron alterados en los EE.UU., por otros programadores, dando origen a muchas versiones de ese virus, cada una de ellas peor que la precedente. Hasta la fecha nadie estaba tomando en serio el fenómeno, que comenzaba a ser bastante molesto y peligroso.

En 1987, los sistemas de Correo Electrónico de la IBM, fueron invadidos por un virus que enviaba mensajes navideños, y que se multiplicaba rápidamente. Ello ocasionó que los discos duros se llenaran de archivos de origen viral, y el sistema se fue haciendo lento, hasta llegar a paralizarse por mas de tres días. La cosa había llegado demasiado lejos y el Big Blue puso de inmediato a trabajar en los virus su Centro de Investigación Thomas J. Watson, de Yorktown Heights, NI.

Las investigaciones del Centro T. J. Watson sobre virus, son puestas en el dominio público por medio de Reportes de Investigación, editados periódicamente, para beneficio de investigadores y usuarios.

El virus Jerusalem, según se dice creado por la Organización de Liberación Palestina, es detectado en la

Universidad Hebrea de Jerusalem a comienzos de 1988. El virus estaba destinado a aparece el 13 de Mayo de 1988, fecha del 40 aniversario de la existencia de Palestina como nación. Una interesante faceta del terrorismo, que ahora se vuelca hacia la destrucción de los sistemas de cómputo, por medio de programas que destruyen a otros programas.

El 2 de noviembre del 88, dos importantes redes de EE.UU. se ven afectadas seriamente por virus introducidos en ellas. Mas 6,000 equipos de instalaciones militares de la NASA, universidades y centros de investigación públicos y privados se ven atacados.

Por 1989 la cantidad de virus detectados en diferentes lugares sobrepasa los 100, y la epidemia comienza a crear situaciones graves. Entre las medidas que se toma, para tratar de detener el avance de los virus, es llevar a los tribunales a Robert Morís Jr. acusado de ser el creador de un virus que infectó a computadoras del gobierno y empresas privadas. Al parecer, este muchacho conoció el programa Core Ware, creado en la AT&T, y lo difundió entre sus amigos. Ellos se encargaron de diseminarlo por diferentes medio a redes y equipos. Al juicio se le dio gran publicidad, pero no detuvo a los creadores de virus. La cantidad de virus que circula en la actualidad es desconocida.

Los virus de computadora son parte real y presente en la cultura computacional. **¡Nos guste o no, tendremos que aprender a convivir con ellos**! En 1995 se creó el primer virus de lenguaje de macros, WinWord Concept.

4.1.4 Vida del virus

Creación.−Hasta unos años atrás, crear un virus requería del conocimiento del lenguaje de programación assembler. Hoy en día, cualquiera con un poco de conocimiento en programación puede crear un virus. Generalmente, los creadores de los virus, son personas maliciosas que desean causar daño a las computadoras.

Gestación.− Luego de que el virus es creado, el programador hace copias asegurándose de que se diseminen. Generalmente esto se logra infectando un programa popular y luego enviándolo a algún BBS o distribuyendo copias en oficinas, colegios u otras organizaciones.

Reproducción.− Los virus se reproducen naturalmente. Un virus bien diseñado se reproducirá por un largo tiempo antes de activarse, lo cual permite que se disemine por todos lados.

Activación.− Los virus que contienen rutinas dañinas, se activarán con ciertas condiciones, por ejemplo, en determinada fecha o cuando el usuario haga algo determinado. Los virus sin rutina dañina no se activan, pero causan daño al robar espacio en el disco.

Detección.− Esta fase por lo general viene después de la activación. Cuando se detecta y se aísla un virus, se envía al International Security Association en Washington D.C., para ser documentado y distribuido a los encargados de desarrollar los productos antivirus. El descubrimiento, normalmente ocurre por lo menos un año antes de que el virus se convierta en una amenaza para la comunidad informática.

Asimilación.− En este punto, quienes desarrollan los productos antivirus, modifican su programa para que éste pueda detectar los nuevos virus. Esto puede tomar de un día a seis meses, dependiendo de quien lo desarrolle y el tipo de virus.

Eliminación.− Si suficiente cantidad de usuarios instalan una protección antivirus actualizada, puede eliminar cualquier virus. Hasta ahora, ningún virus ha desaparecido completamente, pero algunos han dejado de ser una amenaza.

Los virus son muy comunes cuando se baja información de la Internet ya que hay demasiados tipos de virus tanto benignos como malignos, y los virus como ya sabemos son un tipo de archivo ó programas que se ejecuta cada vez que se habré ese archivo sé esta ejecutando el virus, hay unos que se reproducen cada vez que pasa esto, por eso es muy importante tener un antivirus actualizado ya que diario se crean nuevos virus.

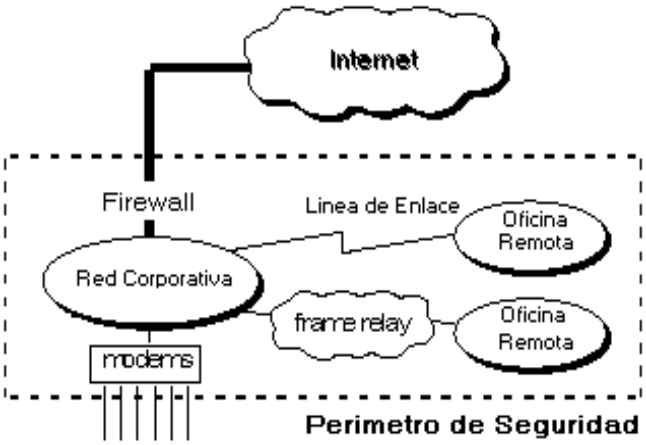
Si el ordenador esta en Red cada vez que se ejecute e l archivo infectado se infectara toda la Red.

4.2 Sistemas de Protección que existen para la Red

4.2.1 Firewalls y seguridad en Internet

La seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el numero de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e−mail), Telnet, y File Transfer Protocol (FTP). Adicionalmente los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso publico en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de su red a los Expertos de Internet (*Internet Crakers*). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no−autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Todavía, aun si una organización no esta conectada al Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.



Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir, quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información.

El firewall podrá únicamente autorizar el paso del trafico, y el mismo podrá ser inmune a la penetración. Desdichadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

Esto es importante, ya que debemos de notar que un firewall de Internet no es justamente un rute ador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información.

Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial−in y dial−out, reglas de enciptacion de datos y discos, normas de protección de virus, y entrenamiento.

Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

4.2.1.1Beneficios de un firewall en Internet

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no−autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser moni toreada y si aparece alguna actividad sospechosa , este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del trafico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado!.

Beneficios De Un Firewall para la Red

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Un firewall es un lugar lógico para

desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re−enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs) .

Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Finalmente, el firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando − únicamente el acceso al Internet esta perdido − .

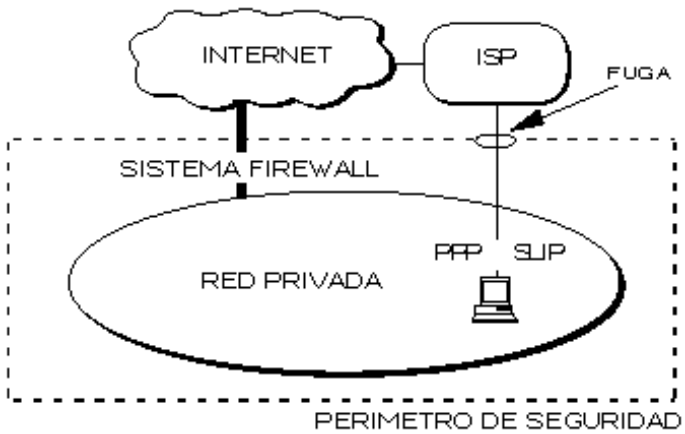
La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significa dos puntos potenciales de ataque a la red interna que tendrán que ser moni toreados regularmente!

4.2.1.2 Limitaciones de un firewall

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

Por ejemplo, si existe una conexión dial−out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet. Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un Firewall Proxy server (FPS) lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque. Los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.



Conexión Circunvecina Al Firewall De Internet.

El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquettes o tarjetas PCMCIA y substraigan estas del edificio.

El firewall no puede proteger contra los ataques de la "Ingeniería Social", por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor del corporativo o que le permita el acceso "temporal" a la red.

Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software. Obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el.

La solución real esta en que la organización debe ser consciente en instalar software anti−viral en cada despacho para protegerse de los virus que llegan por medio de disquettes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparentemente datos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo mas fácil el acceso de un intruso al sistema.

Como nosotros podemos ver, el desempeño de los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles por los ataques con transferencia de datos.

4.2.2 Antivirus

A la hora de escoger antivirus puede aparecer la duda del producto por el que decantarse. El problema más importante de este tipo de software es que siempre va por detrás de su objetivo, el virus informático. Los factores más importantes a la hora de valorar un antivirus son:

4.2.2.1 Capacidad de detección y desinfección

Es lógico. Un antivirus será mejor cuanto más virus sea capaz de detectar y eliminar. Es más peligroso pensar que no se tiene un virus que tener la duda, por ello no hay nada peor que sentirse seguro con un antivirus desfasado o que ofrezca pocas garantías.

4.2.2.2 Heurística

Es la capacidad de detectar virus desconocidos por medio de sondeos del sistema en busca de "síntomas" clásicos de infección como pueden ser fechas extrañas en ficheros, programas residentes en memoria, configuración extraña del sistema (como por ejemplo que Windows 95 tenga activado el modo de compatibilidad MS−DOS), etc. El problema de la heurística es que puede dar "falsos positivos" es decir, puede dar por infectado un fichero que en realidad no lo está.

4.2.2.3 Velocidad

Hoy en día los discos duros son enormes, y si pensamos en intranets y redes corporativas la cantidad de datos a escanear puede ser colosal. Por lo tanto se valorará en un antivirus la capacidad de escanear rápidamente.

4.2.2.4 Actualización

Cada día aparecen cientos de virus nuevos, para que un antivirus sea capaz de eliminar un virus es necesario que incluya la información del virus y su antídoto en las librerías o bases de datos víricas.

La posibilidad de actualizar esas librerías (sobre todo a través de Internet) es un factor fundamental.

4.3 ¿Cuál antivirus elegir?

La expresión "cuál es el mejor antivirus", puede variar de un usuario a otro. Es evidente que para un usuario inexperto, el término define casi con seguridad, al software que más fácil de instalar y usar se le presenta. Algo totalmente intranscendente para usuarios expertos, administradores de redes, etc.

Sin embargo, los usuarios inexpertos también son muy propensos a dejarse influir por lo que las publicaciones especializadas les indican. El tema aquí es que muchas veces este tipo de evaluación no es tan cristalino. No estamos diciendo que algunas publicaciones puedan dejarse influir en sus "Selecciones del editor" por el hecho de que ciertos antivirus son sus clientes y contratan publicidad en sus medios, pero es un tema delicado que de por sí le quita transparencia a ciertas pruebas, por decirlo de algún modo.

También existe el hecho de que algunos reporteros que hacen dichos artículos, no son precisamente expertos en el tema, y por lo tanto sus apreciaciones pueden estar enviciadas por aquello de las apariencias puramente estéticas del producto evaluado, sin entrar en las verdaderas condiciones de un antivirus.

En definitiva, el mejor antivirus debería ser aquel capaz de descubrir y eliminar al 100% de los virus activos ("In−The−Wild"). Esto es lo ideal, pero depende también del usuario, ya que el tener el antivirus actualizado es fundamental.

En estos días de proliferación masiva de ataques de nuevos virus, muchos usuarios de computadoras, se habrán preguntado si ellos tienen la protección adecuada en sus equipos, o dicho de otro modo, si los antivirus que acostumbran usar, los protegen adecuadamente.

Muchas veces se ha dicho que ningún antivirus tiene toda la capacidad de detectar y proteger contra todas las variantes conocidas y por conocer de virus.

Para determinar cuál es el programa antivirus más completo y por ende seguro, se requieren muchos datos de pruebas en las que se puedan confiar, y realizadas a través de un periodo determinado de tiempo.

No es un juicio de valores en el sentido que 2 puntos significa simplemente 2 coincidencias. Lo que usted puede decidir con esto es con cuál antivirus quedarse, si desea tener en cuenta la opinión de una mayor cantidad de expertos.

4.3.1 Comparación de los Antivirus

Datafellows F− Secure:

Es el mejor antivirus existente en el mercado. Tanto que incluso los desarrolladores de virus lo recomiendan y comienzan a desarrollar virus dedicados especialmente a atacar este antivirus, lo cual puede interpretarse como un algo para la gente de Datafellows.

Producto de la unión de F−Prot y AVP combina la potencia de uno con el análisis del otro, ofreciendo un antivirus robusto, rápido y fiable.

Es capaz de escanear redes enteras y su base de datos viral está muy actualizada. Es el antivirus que más virus detecta y elimina, con una heurística muy fiable.

Dr. Solomon's

Un clásico entre los clásicos que sabe mantenerse a la cabeza con poderosas razones. A pesar de no ser tan rápido como el F−Secure el antivirus del Dr. Solomon es capaz de detectar y eliminar gran cantidad de virus y con gran fiabilidad.

Su heurística también esta muy trabajada y en pocas ocasiones dará falso positivos.

Panda Software:

Panda Antivirus Evolución del antiguo Artemis ha sabido mantenerse joven durante todo este tiempo y colocarse entre uno de los mejores. Respetado incluso fuera de nuestras fronteras (Es un producto nacional) cuenta con un servicio de atención 24Hrs 365d y frecuentes actualizaciones. La heurística empeora en comparación con los dos anteriores así como su velocidad.

Anyware: Anyware Antivirus

Pensado tal vez para el usuario doméstico el Anyware parece creer que a este tipo de usuarios el problema de los virus les afecta en menor medida. No hay mucho que comentar en cuanto a este producto.

McAfee: VirusScan

Otro de los grandes clásicos que tampoco ha sabido mantenerse a la altura de las circunstancias. El fallo de este producto es también la falta de actualización de las bases de datos de virus que se centra sobre todo en virus "regionales".

Thunderbyte Antivirus

No es un mal antivirus, el problema es que su heurística es demasiado intransigente. Es quizás uno de los antivirus que más virus ve donde no los hay. Por detectar virus los detecta incluso cuando escaneamos otro antivirus con él.

No apto para cardiacos este producto está bastante dejado por parte de sus programadores, que si bien se llevaron sus elogios al principio merecen ahora una sincera crítica.

Antivirus	Sistemas Operativos probados	Puntaje
Norton Antivirus	DOS/3.x/95/98/2000/NT	14
McAfee (VirusScan)	DOS/95/98/2000/NT	11

Panda Antivirus (Platinum)	3.x/95/98/2000/NT	12
InoculateIT	3.x/95/98/2000/NT	9
Command Software Antivirus	DOS/95/98/NT	7
Norman Antivirus	DOS/95/98/NT	4
PC−Cillin	95/98/NT	3
F−Secure	95/98	3
Sophos Anti−Virus	DOS/3.x/95/98/NT	3

Por los resultados obtenidos en la comparación de los Antivirus el que proporciona mejor servicio es Symantec Norton Antivirus ya que cuenta con mayor definiciones de Virus, aviso de versiones actuales de los virus que salen día con día, también cuenta con herramientas para reparar el sistema y el disco duro, para el Café Internet es importante también implantar un Firewalls esto para estar al tanto de la comunicación de la Red de Área Local.

V. Conclusiones

Con esta investigación se llego a la conclusión de que el mejor programa para la seguridad del Café Internet es Norton Antivirus y las paredes de fuego (firewalls) estas con objeto de supervisar las comunicaciones entre la red de área local.

No existe hoy en día una política antivirus que sea cien por cien efectivo. La forma de evitar desastres es mantenerse al tanto de las ultimas novedades en seguridad informática, sumando una buena gestión del sistema de disco.

Un programa Antivirus por muy bueno que sea se vuelve obsoleto muy rápidamente ante los nuevos virus que aparecen día con día

También es una buena política antivirus evitar la inclusión en el sistema de programas piratas o de procedencia dudosa, ya que son los más susceptibles de estar contaminados.

VI. Recomendaciones

6.1. Recomendaciones para mejorar Su Protección

Seguridad Informática

- Realice backups frecuentes. RECUERDE, el software se puede comprar de nuevo, su información (la de su empresa) SÓLO USTED PUEDE PROTEGERLA, Y SU PÉRDIDA LE OCASIONARÁ GRAVES DAÑOS.
- No olvide proteger y HACER BACKUPS de TODOS los portátiles de la empresa, éstos contienen generalmente información confidencial y valiosa.

Los virus también se extraen de los correos electrónicos, por que hay personas que bajan todo tipo de archivos que les mandan, aquí esta unos puntos, para no infectar su equipo:

- Un e−mail puede incorporar un virus en una macro. Al abrir un mensaje que incluya macros, asegúrese de que las ha desactivado antes de continuar. Tenga configurados sus programas para que le avisen antes de

abrir un archivo que contenga macros. Excel y Word tienen un revisor interno que chequea la existencia de macros.

- Un e−mail puede incorporar un virus en un script de Visual Basic y en HTML. Es muy parecido a las macros. Hay que desactivar la opción de ejecutar los scripts en el navegador o en el procesador de textos.
- Si recibe algún mensaje de alguien a quien no conoce y ese mensaje contiene un archivo adjunto, no lo abra hasta que esté seguro de que el archivo no contiene ningún virus.

Más recomendaciones

- Asegúrese de que los PCs están configurados para arrancar primero siempre desde C: y no desde disquetera. De este modo, estarán protegidos contra infecciones accidentales de virus de boot.
- Proteja contra escritura NORMAL.DOT. Los virus de macro suponen hoy en día más del 90% de las infecciones. La mayoría de los virus de macro de Word atacan infectando el archivo NORMAL.DOT. Al proteger este archivo para que sólo se pueda leer, podrá a detectar todos los intentos de sobrescritura. *Esto no evita infectarse con virus de macro pero sí disminuye los problemas cuando ya se ha producido una infección.*
- Cuidado con los programas gratuitos en Internet.
  Hay muchos programas y herramientas útiles en Internet disponibles, sólo hay que descargarlos, pero muchos de ellos pueden incluir un virus.
  Si consigue algún programa de este tipo, asegúrese de que está limpio antes de utilizarlo.
- Cambie el archivo AUTOEXEC.BAT. Renombre C:\AUTOEXEC.BAT con C:\AUTO.BAT, cambie su archivo C:\AUTOEXEC.BAT a la siguiente línea: *auto* . Si un virus o troyano se suma o reemplaza el archivo AUTOEXEC.BAT, será muy fácil darse cuenta. Si se añade al final del archivo, el código no se ejecutará.
- Distribuya solamente archivos .RTF (en vez de archivos .DOC) Los archivos en formato .RTF no soportan macros. Además, estos archivos ocupan menos que los archivos .DOC por lo que el receptor estará más satisfecho.
- Un método común de introducir virus en una empresa es a través del trabajo traído de casa. Frecuentemente, estos equipos son compartidos por varios miembros de la familia, posiblemente también niños, y hay que tener en cuenta que los colegios son centros de intercambio de programas, con el riesgo que esto conlleva.

NO OLVIDE MANTENER SU ANTIVIRUS ACTUALIZADO

Infección de Virus. Si a pesar de todo, sufre una infección de virus, siga las siguientes recomendaciones:

- Lo primero de todo, EVITAR EL PÁNICO.
- Informar a los responsables de seguridad informática.
- Si se trata de una red, COMPROBAR PRIMERO EL SERVIDOR Y DESPUÉS LAS ESTACIONES DE TRABAJO.
- AISLAR EL PC y evitar el intercambio de disquetes y CD's con otros PC's.
- No enviar mensajes ni archivos a través de la red o de Internet.
- Comprobar que existen BACKUPS ACTUALIZADOS y, si no es así, HACERLOS INMEDIATAMENTE, aunque el PC ya esté infectado.
- Comprobar que está instalada (o instalar) LA VERSIÓN MÁS ACTUALIZADA QUE EXISTA DEL

SOFTWARE ANTI−VIRUS ADECUADO.

Mantenga su antivirus actualizado con toda la frecuencia que le sea posible. Un antivirus por muy bueno que sea SIN ACTUALIZAR NO SIRVE PARA DEFENDERSE ANTE LOS VIRUS DE NUEVA GENERACIÓN.

VII.− Bibliografía

- Siyan Karanjit,1998,La Seguridad en Internet, Prentice Hall, Mexico
- Jischer Jennrich,1995,Internet Interno, Marcombo, España
- http:// www.megazona.com/zonavirus/
- http://www.edata.es/Enciclop.html
- Rolf Oppliger, 1999, Aplicaciones para Seguridad en Redes, Rama, Colombia

ANEXOS

Entrevistas

¿Has oído hablar de los Virus Informaticos?

Muy poco

¿Sabes lo que son?

Pues solo sé que dañan la información

¿Has tenido problemas con tu información a causa de ellos?

Si, una vez estaba imprimiendo mi tarea y después se apago la maquina

¿Conoces alguna forma de prevenir los Virus Informaticos y Cuáles son?

Solamente con los programas, que le llaman Antivirus

¿Crees que te serviría si colocamos información acerca de los Virus Informaticos?

La verdad, es que me seria muy útil.

¿Has oído hablar de los Virus Informaticos?

Poco

¿Sabes lo que son?

Sé que son programas que dañan los archivos

¿Has tenido problemas con tu información a causa de ellos?

No ,nunca

¿Conoces alguna forma de prevenir los Virus Informaticos y Cuáles son?

La vedad no lo sé

¿Crees que te serviría si colocamos información acerca de los Virus Informaticos?

Pues si, para saber que son

¿Has oído hablar de los Virus Informaticos?

Sí

¿Sabes lo que son?

Son programas malos dentro de la computadora

¿Has tenido problemas con tu información a causa de ellos?

Solamente una vez

¿Conoces alguna forma de prevenir los Virus Informaticos y Cuáles son?

Solo el Antivirus

¿Crees que te serviría si colocamos información acerca de los Virus Informaticos?

Si, estaría muy bien para saber todo acerca de los virus

¿Has oído hablar de los Virus Informaticos?

Sí

¿Sabes lo que son?

Se que producen mucho daño a la información y que se extiende muy rápido

¿Has tenido problemas con tu información a causa de ellos?

No

¿Conoces alguna forma de prevenir los Virus Informaticos y Cuáles son?

Los Antivirus

¿Crees que te serviría si colocamos información acerca de los Virus Informaticos?

Pues serviría muy bien, así para saber acerca de los últimos virus que salgan

¿Has oído hablar de los Virus Informaticos?

Poco

¿Sabes lo que son?

Solo sé que son malos

¿Has tenido problemas con tu información a causa de ellos?

No

¿Conoces alguna forma de prevenir los Virus Informaticos y Cuáles son?

Con un Antivirus

¿Crees que te serviría si colocamos información acerca de los Virus Informaticos?

Si para saber como prevenirlos

¿Has oído hablar de los Virus Informaticos?

Sí

¿Sabes lo que son?

No

¿Has tenido problemas con tu información a causa de ellos?

Si

¿Conoces alguna forma de prevenir los Virus Informaticos y Cuáles son?

Con las Vacunas

¿Crees que te serviría si colocamos información acerca de los Virus Informaticos?

Si, demasiado

¿Has oído hablar de los Virus Informaticos?

Sí

¿Sabes lo que son?

Son programas que dañan la información

¿Has tenido problemas con tu información a causa de ellos?

Si

¿Conoces alguna forma de prevenir los Virus Informaticos y Cuáles son?

Los Antivirus

¿Crees que te serviría si colocamos información acerca de los Virus Informaticos?

Si mucho

¿Has oído hablar de los Virus Informaticos?

Si

¿Sabes lo que son?

Si, son programas que hacen daño a la computadora

¿Has tenido problemas con tu información a causa de ellos?

Sí

¿Conoces alguna forma de prevenir los Virus Informaticos y Cuáles son?

Si, con los antivirus

¿Crees que te serviría si colocamos información acerca de los Virus Informaticos?

Si

¿Has oído hablar de los Virus Informaticos?

Sí

¿Sabes lo que son?

Son archivos que dañan información de las maquinas

¿Has tenido problemas con tu información a causa de ellos?

Si

¿Conoces alguna forma de prevenir los Virus Informaticos y Cuáles son?

Pues lo más común son los antivirus pero también existen Firewalls

¿Crees que te serviría si colocamos información acerca de los Virus Informaticos?

Si para saber los virus que se descubren cada día.

XXIX