PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN CENTRAL Y UNIFICADA SOBRE SEGURIDAD EN AMBIENTES MICROSOFT EN EL LABORATORIO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (LTIC) DE LA FACULTAD DE INGENIERÍA."

AUTOR:

HUGO RENE PAREDES VALDIVIESO

DIRECTOR: ING. FRANCISCO RODRIGUEZ

QUITO, 2010

Tabla de Contenido

Introducción.

En actualidad existe gran facilidad para mantener contacto mediante la tecnología los más privilegiados tienen acceso a conectarse a la extensa red de información llamada Internet debido a esta facilidad de acceso es indispensable estar protegido contra las amenazas que intentan aprovechar cualquier vulnerabilidad disponible para robar o dañar nuestra información o privacidad de forma fraudulenta.

No cabe duda que existe conciencia hacia la importancia de tener nuestros sistemas protegidos pero no siempre se invierte el tiempo ni los recursos a la misma ya que lo primordial es que el sistema esté listo para nuestro trabajo diario, pero cuando el sistema falla o cae bajo ataques es en verdad cuando se toman las medidas correspondientes.

Así es como la pregunta viene a discusión “¿Es importante invertir en la seguridad de nuestros sistemas?”. Parece una respuesta fácil de responder pero no muchas veces se lleva a la práctica la respuesta si es afirmativa.

Si tomamos el ejemplo del propietario de una casa que hace lo necesario para cerrarla y mantenerla alejada de personas inescrupulosas que podrían atentar contra ella o contra sus habitantes. Entonces, ¿Por qué no hacer lo mismo con nuestros sistemas informáticos? si nuestros sistemas informáticos son los que guardan nuestra información importante y son de base en el funcionamiento de las organizaciones.

Sin embargo, la falta de conocimiento o rigor al administrar una red, ha provocado que no se apliquen adecuadamente las medidas de control y seguridad, aun disponiendo de medios para ello, si a lo anterior sumamos la complejidad creciente de las infraestructuras de red, el poder encontrar una solución unificada, integrable, sencilla y ágil, que permita visualizar información de forma centralizada, donde un solo vistazo permita conocer el estado de seguridad de la infraestructura, mediante reportes gráficos, con información detallada, de

fácil acceso, permite a los encargados de TI de las organizaciones manejar de mejor manera los recursos disponibles.

Pero ahora no solo basta con adquirir o disponer de un sistema de seguridad para sentirnos confiados o medianamente seguros debido a que un sistema por sí solo no soluciona todos nuestros problemas de seguridad, un sistema seguro también depende de un conjunto de reglas, planes y acciones que permitan asegurar la continuidad de la organización o negocio. Se debe tener en cuenta que se tiene múltiples objetivos a cumplir, dedicar cierto esfuerzo a la instalación y configuración de los componentes de dicho sistema, sea este de hardware o software. Así como en manejar políticas de seguridad como de acceso solo a usuarios autorizados, complejidad de claves, etc.

Antes de realizar cualquier implantación de cualquier sistema de seguridad se debe indicar a las personas que lo van a utilizar que se va a partir siempre de una premisa básica:

"No existe el 100% de seguridad y es imposible lograr ese nivel de protección"

Pero si podremos lograr que el sistema utilice las mejores prácticas de seguridad posibles en la organización u institución para mantener un buen nivel de seguridad.

Existen amenazas y debilidades comunes a las que todo sistema está expuesto por el simple hecho de utilizar un medio informático y es importante tener en consideración estos puntos según el sistema operativo utilizado para minimizar los riesgos a un nivel aceptable.

La mayoría parte de los conceptos y acciones tomadas en consideración son para una plataforma PC utilizada en ambientes Microsoft Windows, debido a que la principal plataforma usada no solo en el LTIC sino también en la gran mayoría de organizaciones e instituciones es Microsoft Windows. Pero se utilizaran lineamientos básicos que muy bien pueden ser utilizados en otros sistemas operativos distintos al mencionado.

En una infraestructura donde la mayor cantidad de usuarios son estudiantes se produce una problemática de seguridad en los equipos clientes, ya que el malware y sus variantes, no se pueden detener no sólo con un antimalware, sino que también se necesita las respectivas actualizaciones de seguridad para los mismos que son publicadas por los fabricantes de los sistemas operativos y otras variables que pueden afectar la integridad de la infraestructura de la organización como por ejemplo la Ingeniería Social.

Los beneficios al obtener un sistema de gestión central y unificada de seguridad fácilmente administrable, que aprovechen una integración nativa con la tecnología Microsoft que es la principalmente utilizada en el LTIC, hacen que la implantación sea de manera transparente tanto para administradores y usuarios así la herramienta la cual permitirá:

Protección unificada: Con una respuesta efectiva contra malware actual y tradicional en tiempo real, que tiene un respaldo de múltiples fuentes de datos las cuales llevan una investigación de seguridad global permanente.

Administración simplificada: A través de una administración central mediante una consola para la administración de seguridad simplificada, ahorrando tiempo y reduciendo complejidad. Utilizando interfaces familiares, donde es fácil visualizar y desplegar configuraciones tales como:

- Definir políticas para administrar grupos de computadores mediante los agentes desplegados en los computadores cliente donde también se puede incluir niveles de alerta.
- Implementar actualizaciones de seguridad y firmas de seguridad en forma más rápida en los sistemas operativos Microsoft de escritorios, computadoras portátiles y servidores.
- Integrar con la infraestructura de red actual mediante la integración con el software de infraestructura existente.

Control y visibilidad: Mediante la producción de reportes de seguridad, de modo que con una sola captura de pantalla permita visualizar el estado actual de seguridad de la infraestructura, ayudando al administrador a tomar un control sobre las amenazas de malware y comprender dónde se requiere la acción, ya sea de forma inmediata o mediante un análisis del problema que está causando el inconveniente de seguridad, todo mediante informes en tiempo real.

Por lo tanto, un sistema de gestión central y unificada de seguridad, que tiene la capacidad de aplicarse en la red del LTIC puede aprovecharse para mantener el funcionamiento del Laboratorio y poder mantener sus prestaciones para todos los usuarios del mismo.

Capítulo 1: Vulnerabilidades de la Seguridad.

¿Qué es seguridad?

Podemos entender como seguridad a la característica de cualquier sistema sea informático o no, que nos indica que ese sistema está libre de todo peligro, riesgo, de cierta forma infalible.

Particularizando para el caso de los sistemas informáticos, los cuales entre sus componentes tienen hardware, software, sistemas operativos y redes. Es complicado para los administradores del sistema conseguir que el sistema sea infalible debido a que los sistemas van creciendo en conjunto con la organización lo cual los hace mucho más complicados de administrar. Pero acercando la definición más hacia la realidad, un sistema no puede llegar a ser infalible, ya que el único sistema que encajaría en esa definición es uno apagado debido a que el único ataque del que sería víctima seria de un daño físico.

Así, es como podríamos decir que un sistema seguro es un sistema fiable, ya que un sistema fiable funcionan de acuerdo a como el administrador desea, esto se podría definir

así debido a que gran parte del Software Maliciosos que atacan a nuestros sistemas buscan no solo tomar información sino también evitar que el sistema funcione bien.

Todo sistema seguro de forma más general busca cumplir básicamente con principios para garantizar su funcionamiento como lo son la confidencialidad, integridad, disponibilidad y privacidad.

- **Confidencialidad:** Se enfoca en la información y la necesidad de que la misma sólo sea conocida por personas autorizadas.
- **Integridad:** Enfocada también en la información y es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado.
- **Disponibilidad:** La capacidad de estar siempre disponible y en el caso de la información estar disponible para ser procesada por las personas autorizadas.
- **Privacidad:** Derecho de mantener en secreto nuestras acciones, los datos personales y nuestras comunicaciones.

Pero los puntos definidos anteriormente dependen también del entorno o sistema donde están operando cada uno ya que un punto puede tomar más importancia que el otro.

Por ejemplo, en un sistema de la milicia se antepondrá la confidencialidad de los datos almacenados o transmitidos sobre su disponibilidad, debido a que es preferible que alguien borre información confidencial (Fácilmente recuperable después en un backup) a que ese mismo atacante pueda leerla o a que esa información esté disponible en un instante dado para los usuarios autorizados.

Por otro lado en un entorno bancario, la prioridad del sistema es la integridad de los datos frente a su disponibilidad o su confidencialidad es menos delicado si un cliente del banco consigue leer el saldo de otra persona que el hecho de poder modificar el saldo.

1.1 Amenazas Actuales

En la actualidad existe una gran variedad de amenazas a las que el usuario de un sistema operativo está expuesto, ya que los ataques son diversos y provienen de distintas fuentes, su forma de propagación cambia día a día e incluso sin ser necesariamente un software malicioso, los mismos ya no solo están centrados en equipos miembros de una red sino que también se pueden ver expuestos equipos que utilizan dispositivos extraíbles que utilizamos diariamente.

El origen de lo que conocemos comúnmente como "Virus Informáticos" ha ido evolucionando a la par del desarrollo de todos los sistemas informáticos. Es así como los primeros virus utilizaban los medios disponibles para reproducirse como lo fueron los disquetes los cuales tenían un menor impacto y velocidad de reproducción ya que si no llegaba el medio físico al usuario este no podía contagiarse.

Pero luego con la masificación de las redes y la llegada del internet los virus tuvieron su oportunidad para propagarse de forma exponencial y llegar a cualquier parte del mundo sin la necesidad de utilizar medios físicos directamente.

Debido a que el desarrollo malware ha ido cambiando con el tiempo y ya no solo es conocido con este nombre sino que también debido a sus evolución en la historia se vio la necesidad de realizar una clasificación del mismo por que actúa de forma diferente y con diversos fines de acuerdo a su clasificación.

1.2 Historia de Malware[1]

Desde que el hombre empezó a automatizar sus actividades con artefactos mecánicos, aparecieron las primeras máquinas que ya podían procesar información y no solo realizar actividades mecánicas. Debido a este desarrollo no solo aparecieron procesos que ayudaban a sus creadores sino también procesos que tenían la intención de afectar estos procesos de ayuda ya creados. Es así como el malware está ligado desde la creación de los primeros programas de computadora.

1.2.1 Génesis: 1800 A 1960

El primer intento de automatizar procesos fue realizado con máquinas analógicas, es así como en 1931 Vannevar Bush construyo su analizador diferencial en el MIT (Instituto Tecnológico de Massachussets), conocida como la primera computadora analógica la cual podía realizar automáticamente algunas de las operaciones elementales, en este mismo año el matemático inglés George Boole describió el álgebra que lleva su nombre la cual dio origen a la ciencia de la computación.

Pero quien empezó la idea de unir el mundo mecánico con la información fue Claude Elwood Shannon, quien en su tesis de licenciatura, estableció el paralelismo entre la lógica de Boole y los circuitos de transmisión. Después del apogeo de nuevas propuestas e ideas acerca del desarrollo estas máquinas lógicas empezó con la creación de las primeras computadoras electromecánicas digitales dando paso a la construcción de primera computadora decimal ENIAC finalizada en 1946.

---

[1] Texto tomado de: BORGHELLO, Cristian. *Cronología de los virus informáticos: historia del malware*. [en línea].ESET Latinoamérica, 14/11/2006, 4/12/2009, [citado 10-01-2009], Formato pdf, Disponible en Internet: http://www.eset-la.com/press/informe/cronologia_virus_informaticos.pdf

Para el año de 1947, se da un gran salto teórico tecnológico: los premios Nobel John Bardee, Walter Brattain y William B. Shockley diseñan el transistor, con el cual comienza la substitución de los tubos de vacío, disminuyendo drásticamente el volumen de las máquinas.

Es así como en 1951, se da el origen a las primeras computadoras fabricadas comercialmente con la UNIVAC I, primera en utilizar un compilador para traducir un programa en lenguaje máquina. Y después la lista siguió con otras creaciones importantes en el avance de la tecnología de la computación como:

- En 1954 IBM 650 construye la primera computadora de producción masiva habiendo 100 de ellas en el mundo.
- En 1957 nace el primer lenguaje de programación de alto nivel, FORTRAN, desarrollado por la empresa IBM (International Business Machine).
- En 1959, el premio Nobel Jack S. Kilby, empleado de la compañía informática estadounidense Texas Instruments, desarrolla el microchip.
- En 1964, IBM anuncia el lanzamiento del Sistema/360, primera familia de computadoras compatibles, llevado a John Kemeny y Thomas Kurtz a desarrollarar el BASIC[2] dando paso al origen de los lenguajes de programación modernos.

Luego de la aparición de la Apple I primera PC de uso masivo, presentada en 1976 y en 1977. En 1981, IBM establece un estándar con su primer PC de propósito general y distribuido con el sistema operativo PC-DOS (MS-DOS de la naciente Microsoft), el cual fue adoptado en relación de otros Sistemas Operativos presentes a la época como el CP/M de Gary Kildall. El MS-DOS es un clon de QDOS (Quick and Dirty OS de Tim Paterson) (a su

[2] Beginners All-purpose Symbolic Instruction Code

vez clon de CP/M), el cual William Henry Gates III (Bill Gates) compro y le realizo pequeñas modificaciones antes de llegar a un acuerdo con IBM.

1.2.2 Prehistoria: 1948 - 1983

Inspirados en la teoría de las "máquinas de Von Neumann" capaces de reproducirse a sí mismas en pro de un objetivo común en los laboratorios de la Bell Computer, tres jóvenes programadores: Robert Thomas Morris, Douglas Mcllroy y Victor Vysottsky crean un juego denominado CoreWar[3]

CoreWar juego donde programas combaten entre sí con el objetivo de ocupar toda la memoria de la máquina eliminando y así terminando con los oponentes. CoreWar fue utilizado como entretenimiento para intelectuales durante muchos años y manteniéndose en el anonimato hasta el año 1984 en el cual Ken Thompson[4] lo expone al momento de recibir el premio Turing de A.C.M. (Asociation of Computing Machinery), e insta a la comunidad de esa época a experimentar con estas aplicaciones, dando paso a la creación de la llamada Core War Society (ICWS), la cual actualizó las reglas del juego con las que actualmente se sigue jugando en Internet.

El que se considera el primer virus propiamente dicho y que era capaz de "infectar" máquinas, fue el que afectó a las maquinas del modelo de IBM 360 a través de la red ARPANET (precedente de la Internet), a esta aplicación se la bautizado Creeper, creado en 1972 por Robert Thomas Morris. Este parásito emitía un mensaje en la pantalla periódicamente: "I´m a creeper… catch me if you can!". Traducido al español: "Yo soy creeper … atrápame si puedes!". Para su eliminación se creó otro virus llamado Reaper el

---

[3] Conocido como el precursor de los virus informáticos
[4] Creador del sistema operativo Unix y el lenguaje de programación B

cual fue programado para buscarlo y eliminarlo. Dando paso a los primeros intentos e ideas de creación de lo que ahora conocemos como antivirus.

En enero de 1975, John Walker (fundador de Autodesk) descubre una nueva forma de distribuir un juego en su UNIVAC 1108 e inadvertidamente da origen al primer troyano de la historia. El mismo recibe el nombre “Animal/Pervade”; Animal consistía en un software el cual pedía al usuario adivinar el nombre de un animal en base a preguntas realizadas y Pervade era una rutina capaz de actualizar las copias de Animal en los directorios de los usuarios cada vez que el mismo era ejecutado, de allí que sea un troyano.

Debido a esta forma de auto-actualización, el programa tenía la capacidad de “aprender” de sus errores sobrescribiéndose a sí mismo cada vez que se “equivocaba”. Sin embargo, un error en la programación del juego hacía que existieran múltiples copias de sí mismo en diversos directorios de la máquina. La solución fue crear una versión del juego que buscara versiones anteriores y las eliminara.

A finales de los setenta, John Shoch y Jon Hupp, investigadores del Centro de Investigación Xerox de Palo Alto, California intentaron darle un uso práctico a los CoreWars, creando un programa que se encargara de las tareas de mantenimiento y gestión nocturnas, propagándose por todos los sistemas del centro. Lamentablemente, este “trabajador virtual” bautizado como worm se extendió por toda la red y causó grandes problemas, por lo que se debió realizar la eliminación completa del mismo.

1.2.3 Década 80

En esta década debido a la rápida evolución de las PC y su popularidad, cada vez existían más personas involucradas en la informática las cuales escribían sus propios programas, dando paso al origen de los primeros desarrolladores de programas dañinos.

Es así como para el año 1981, Richard Skrenta recibe una Apple II como regalo y escribe el primer virus de amplia reproducción: Elk Cloner el cual se almacenaba en el sector de inicio de los disquetes de 360 kb y era capaz de residir en memoria luego que el disco era

retirado. Elk Cloner no afectaba al sistema pero contaba la cantidad de arranques y cuando llegaba a cincuenta mostraba las siguientes frases:

Elk Cloner:

The program with a personality

It will get on all your disks

It will infiltrate your chips

Yes it's Cloner!

It will stick to you like glue

It will modify ram too

Send in the Cloner!

Con la velocidad en desarrollo y avance de la tecnología el Sistema Operativo provisto por IBM (MS-DOS) el mismo padecía de grandes agujeros inseguros que permitieron la aparición de códigos maliciosos y su rápida expansión.

Debido a esto se empezó con el estudio de los códigos maliciosos que eran cada vez más comunes y creados por distintas personas.

Así en 1984, Frederick B. Cohen publica sus estudios con el nombre de "Computer Viruses - Theory and Experiments", donde define por primera vez a los virus. Esta definición propuesta por Cohen y que fue aceptada por la comunidad es:

"Programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí mismo"

Por ser el precursor del estudio de los códigos maliciosos, Cohen es conocido como el "Padre de los virus" aunque no fue el primero en trabajar sobre ellos. En este documento también sentó las bases de los programas para combatir a estas amenazas y demuestra que "no hay ningún algoritmo general que pueda concluir con total fiabilidad (100%) si un programa es o no un virus".

Para ello se valía de la siguiente demostración por reducción al absurdo:

“Supóngase que existe un algoritmo general A que, analizando cualquier programa P ,devuelve "true" si y sólo si P es un virus. Entonces sería posible crear un programa P, que hiciera lo siguiente:

si (A(P) = falso) entonces

infectar el sistema

si (A(P) = verdadero) entonces

no infectar

Es decir: P es un virus si A dice que no lo es, y no lo es si A dice que lo es. Por contradicción, ese algoritmo general A no existe.”

Además, Cohen menciona las posibles formas de detección de un virus y las clasifica en:

- Detección por apariencia
- Detección por comportamiento
- Detección por evolución de otros virus conocidos
- Detección por mecanismos de engaño

Cohen no se equivocó, al realizar esta clasificación, ya que la misma es utilizada actualmente por los antivirus modernos. Tampoco equivocó al dar como conclusión que para estar seguros contra un ataque viral, el sistema debe proteger el flujo de información que ingresa y que sale del mismo.

Para el año de 1988, Leonard Adleman en su artículo “An Abstract Theory of Computer Viruses” Adleman introduce el concepto de Cuarentena y lo define como “un sistema aislado para la ejecución programas antes de introducirlos en un ambiente donde hagan daño”. Además incluye el término desinfección, y definiéndolo como “un procedimiento capaz de volver un programa infectado a su estadio anterior a la infección”; y certificación “que asegure que un programa determinado no está infectado”.

En el mismo documento también se define formalmente el término troyano como “programa alojado dentro de otra aplicación, u otro elemento de apariencia inocente, que se instala en el sistema al ejecutar el archivo que lo contiene”.

Después de estos primeros estudios y definiciones entregadas por Cohen y Adleman, se produjeron como era de esperase gran variedad de código malicioso, los cuales poseían distintas formas comportamiento e infección como:

En el año de 1986, se detectó la primera epidemia de un virus totalmente compatible con los IBM PC. El causante fue un virus bautizado Brain, era capaz de infectar la zona de arranque, cambiar el nombre del disco a “(c) Brain” e incluía una línea de texto que contenía los nombres de los programadores, direcciones y número de teléfono.

Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730

NIZAM BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE:

430791,443248,280530.

Beware of this VIRUS.... Contact us for vaccination...

Este programa sólo era un experimento antipiratería según los creadores que los hizo famosos a ellos y a su empresa Brain Computer Services. Esto puede ser confirmado al ver que el virus no contenía carga dañina en su código.

En 1987, dio paso a la aparición del primer virus capaz de infectar Macintosh el bautizado MacMag, también conocido como Brandow, Drew y MacPeace, fue escrito y diseminado a finales de 1987 y principios de 1988. Sus desarrolladores fueron los editores de la revista de computación canadiense “MacMag”. El virus fue distribuido a través de los disquetes que se entregaban a los miembros del Club Mac. Este virus se limitaba a presentar un mensaje de paz en pantalla y al llegar el 2 de Marzo de 1988 (fecha del aniversario de la aparición del Macintosh II), se auto eliminaba.

En 1988, es encontrado en la Universidad de Turín el virus Ping Pong, el cual mostraba en pantalla un pelotita que rebotaba mientras infectaba la zona de arranque del disco. Versiones posteriores de este virus eliminaron el efecto visual y perfeccionaron las formas de infección.

En 1989, fue el año de lanzamiento de la denominada “fábrica búlgara de virus” con el escritor Dark Avenger (o Eddie) a la cabeza, el cual es reconocido como uno de los más prolíficos creadores de virus con técnicas originales.

1.2.4 Década 90´s

En 1990, con la creciente inventiva búlgara, aparece la primera VX-BBS de intercambio de virus, permitiendo descargar cualquier virus siempre y cuando se haya dejado alguno previamente. Esto también marca la importancia de la diferencia entre el desarrollo y la propagación de virus.

Mark Washburn, basándose en el virus Vienna, crea Chameleon el cual era capaz de mutar con cada infección (polimórfico). Esta característica hizo que los algunos antivirus basados en detección por firma resultaran inútiles y los obligara a replantear sus tecnologías, por ejemplo hacia la heurística.

En diciembre de ese año se funda **EICAR (European Institute for Computer Antivirus Research)** en Hamburgo, Alemania. Este instituto es el autor del archivo “EICAR” mismo que tiene la finalidad de probar la eficacia de un antivirus sin involucrar el riesgo de trabajar con un virus real.

El archivo contiene el siguiente código:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

En 1991, se hace evidente que las técnicas para nombrar a los virus son demasiadas confusas por lo que se crea **CARO (Computer Antivirus Research Organization)** para solucionar este problema. La organización original estaba formada por Fridrik Skulason

(Editor de Virus Bulletin y autor F-Prot), Alan Solomon (S&S International) y Vesselin Bontchev (Universidad de Hamburgo).

CARO decide que los virus deben bautizarse de la siguiente forma:

Family_Name.Group_Name.Major_Variant.Minor_Variant[Modifier]

(Prefijo.Nombre.Variante)

Si bien esta nomenclatura se sigue respetando, aún hoy en día la problemática del nombre que reciben los virus sigue vigente.

Para el mes de marzo de 1992, hace la aparición de Michelangelo (virus de arranque, variante de Stoned) es una fecha recordada en la historia, ya que los virus informáticos son masivamente expuestos a la opinión pública. Michelangelo si bien no era un virus peligroso, sus efectos fueron magnificados por la prensa y dispararon la venta de antivirus.

Por otra parte, las capacidades de Dark Avenger seguían creciendo y este virus dio origen a varios motores automáticos de creación de virus.

El primero de éstos fue el MtE (Self Mutating Engine) creado por el mismo Dark Avenger el cual incluía un manual de uso.

Casi a la par aparece Peach, primer virus capaz de “atacar” la base de datos de un antivirus y EXEBug capaz de controlar la CMOS para prevenir el booteo desde disquetes limpios.

En 1993, el experto antivirus Joe Wells había recolectado información sobre la evolución de los virus en el mundo real y en julio de 1993 crea una lista con 104 virus denominada WildList. Actualmente esta lista cuenta con la participación de 80 investigadores de todo el mundo.

Microsoft lanza su propio antivirus: Microsoft AntiVirus (MSAV), basado en Central Point AntiVirus (CPAV). Si bien este antivirus no volvió a aparecer en las versiones sucesivas de los sistemas operativos de Microsoft, no sería este el último intento de empresa por entrar en este mundo, ya que después desarrollo soluciones como Microsoft Forefront Client

Security, Microsoft Windows Live OneCare, Windows Defender y Windows Live Safety Center.

En 1994, entre lo más destacado de este año se encuentra la sentencia a 18 meses de prisión de Christopher Pile (alias Black Baron) por parte de Scotland Yard en Inglaterra. Pile fue acusado de ser el autor de los virus Pathogen, Queeg y del generador SMEG. Esta año fue impórtate debido a que creo un precedente, ya que fue la primera vez que un escritor de virus es acusado legalmente y sentenciado.

En 1995, con el lanzamiento de Windows 95 aparecen nuevos conceptos de infección, así es como Sarah Gordon descubre Concept, mismo que infectó a miles de documentos de Microsoft Word. Concept es conocido como el primer virus de macro escrito en el lenguaje WordBasic de Microsoft y capaz de infectar cualquier plataforma que ejecutara MSWord (PC y Mac).

La proliferación de este virus fue tal que llegó a ser el más común en el mundo durante un largo período de tiempo y de la cual se detectó cientos de variantes.

Para el mes de febrero de 1997 aparecen Staog (escrito en Assembler por el grupo Quantum/VLAD) y Bliss, los primeros virus para archivos ELF del sistema operativo Linux, incluso puede ser compilado para SunOS, Solaris y OpenBSD sin problemas.

En 1998, aparecen BackOrifice, NetBus, Phase y D.I.R.T.; troyanos diseñados como herramientas de administración remota que permitían ser instalados sin conocimiento ni consentimiento del usuario.

Aunque lo más destacable de este año fue sin duda el virus creado por el taiwanés CIH (iniciales de su autor, el estudiante Chen Ing-Hou) o Chernovyl detectado en junio y activado 26 de abril de año siguiente (aniversario del accidente en Chernobyl) o el 26 de cada mes, según la versión.

Este estudiante manifestó en repetidas ocasiones que “siente mucho el daño de su creación viral, pero fue motivado por una venganza en contra de los incompetentes desarrolladores

de software antivirus". Chen fue acusado de esparcir su creación y en septiembre de 2000 fue declarado culpable por la justicia de su país.

Lo que hacía a CIH fue tan especial y realmente muy diferente a lo que realizaban otros virus ya que podía afectar al hardware, su rutina borraba los primeros 2048 sectores del disco rígido y sobrescribía algunos tipos de Flash-Bios dejando inutilizable la placa madre de la computadora.

A principios de 1999 año surge el troyano Happy (conocido como Ska en mención a su autor, el francés Spanska), estrenando una nueva moda que persiste hasta el día de la fecha: los gusanos para MS Outlook. Happy se caracteriza por su mensaje "Happy New Year 1999 !!" y sus fuegos artificiales. Debido a su capacidad de modificar ciertos archivos del sistema es capaz de enviarse a sí mismo a cada persona a quien el usuario envía un correo.

Para marzo del mismo año Melissa comenzó a llegar a miles de correos en un archivo adjunto el cual aparecía enviado por un contacto conocido. Este virus fue el encargado de desechar la idea de que es una buena práctica de seguridad: "no abrir mensajes de personas desconocidas", ya que el virus se adjuntaba en correos de contactos de confianza. La forma de infectarse era muy fácil ya que cuando se abre el archivo adjunto con Word 97 o 2000 con el virus de macro este se activa ,abre Outlook ,y después se auto envía a los primeros cincuenta contactos de la libreta de direcciones. Estas personas reciben un documento infectado de alguien conocido y continúa la cadena. El archivo que se adjunta puede ser cualquiera que el usuario tenga en su sistema, así el virus compartía información confidencial. Melissa utilizo la confianza del usuario en quien le enviaba el correo e hizo que este macro virus se convirtiera en una epidemia rápidamente y causara grandes pérdidas económicas.

Para el mes de diciembre, aparece Babylonia, este virus muy complejo fue el primero en explotar la auto actualización de nuevas versiones de sí mismo desde Internet, practica muy común por los virus de hoy en día.

1.2.5 Década Actual

En el año 2000, conocido como el del fin del mundo informático, aunque no se dio, fue el año que dio inicio a una variedad de avances importantes en lo que a malware se refiere. En este año se hiso popular un generador de gusanos, conocido como VBSWG (Visual Basic Script Worm Generator). Uno de los mejores ejemplos de virus creados por este software fue el virus bautizado Anna Kournikova, que incluso llegó a infectar a la NASA.

Otra de las creaciones recordadas de este año fue la aparición del “gusano del amor” :LoveLetter. El cual llegaba por correo con un adjunto y su nombre se debe a que el asunto del mensaje era “ILOVEYOU”. Los daños ocasionados por este gusano se calcularon en millones de dólares en pérdidas y de máquinas infectadas.

Año 2001.

Estuvo marcado por la proliferación de gusanos que usan combinaciones de vulnerabilidades para su expansión, una fórmula ampliamente utilizada en la actualidad.

En enero nace Ramen y en marzo Lion, gusanos para el sistema operativo Linux, que aprovechan diversas vulnerabilidades en RPC, wuftpd y BIND.

En Suecia en marzo aparece el gusano polimórfico Magistr utilizando rutinas de envío SMTP propias evitando así la utilización de clientes de correo. Era un virus muy completo por la utilización de ingeniosas técnicas y capacidades de propagación, ya que generaba mensajes con asuntos diferentes cada vez y poseía capacidades de destrucción similares a CIH (eliminación de CMOS, la Flash BIOS e información almacenada en el disco).

Para el mes de julio aparece CodeRed el cual se propaga buscando servidores con IIS 5.0 (Internet Information Server) vulnerables. Cuando encuentra un servidor, el gusano intenta ingresar al sistema a través del puerto 80 explotando una vulnerabilidad. Este es otro caso

en donde si bien la actualización por parte de Microsoft ya existía, el gusano continuó su expansión debido a la irresponsabilidad de los administradores.

Según algunos datos estadísticos, CodeRed logró infectar 80.000 servidores en las primeras horas de la fecha de su ataque y llegó a duplicar su área de propagación cada 37 minutos. Esto sólo sería superado por Slammer dos años después.

También en para el mes de julio, el troyano SirCam, escrito en el lenguaje Borland Delphi, es capaz de enviarse a sí mismo a todos los usuarios de la libreta de direcciones de Windows, y a direcciones encontradas en los archivos temporales de Internet, además de aprovecharse de los recursos compartidos y de contener una peligrosa rutina de destrucción. La forma más común de identificarlo era su asunto en español “Hola como estas?”.

En septiembre aparece el troyano Nimda (admin. de administrador de lectura invertida) que se propaga por correo al visualizar páginas web ,a través de recursos compartidos y atacando servidores web (ISS de Microsoft). Una consecuencia directa de la gran propagación de este gusano es la ralentización de la red, debido al gran tráfico generado buscando otros servidores vulnerables.

Se suma una nueva forma para propagar malware: aparecen Hello y Choke, gusanos que se aprovechan del programa MSN Messenger de Microsoft para lograr su objetivo.

Como ataques en otro contexto que al parecer no utilizaban ningún tipo de código malicioso ,en mayo aparece el bautizado hoax (mensaje de correo de correo electrónico falso) en el que se alerta acerca que un programa (sulfnbk.exe) es un peligroso virus.

Este mensaje daba instrucciones precisas para eliminar este archivo si el mismo era hallado. El caso es que este archivo efectivamente siempre era encontrado porque pertenece a Windows. Al eliminarse algunas capacidades del sistema operativo dejaban de funcionar.

El correo lucía de la siguiente forma:

Este VÍRUS no tiene vacuna. Lo acabo de recibir… y estaba en mi computador. Busca en tu computador el archivo: sulfnbk.exe (lo tenía en mi casa - y ya lo borre!, o sea que no puedo pasarlo de nuevo). Anda al menú iniciar ,localizar (o find) y localiza este archivo y bórralo inmediatamente (en caso de que lo encuentres, se aloja en c:/windows/command). Después de esto bórralo también de la papelera. Se trata de un virus que viene a través de e-mails sin que te des cuenta y va a destruir tu computador el día 01.

Linux tampoco estuvo a salvo este año. Aparecen Ramen y Lion, gusanos que explotan distintas vulnerabilidades de sistemas Red Hat.

Año 2002

En enero de este año aparece el primer virus capaz de infectar Macromedia Shockwave Flash (archivos .SWF) y programado en ActionScript.

En el día de los enamorados se marca la aparición de Yaha (o Lentin o San Valentín) un falso protector de pantalla de San Valentín. Debido a esta técnica de engaño logró una propagación masiva.

En mayo el gusano Spida comienza a aprovecharse de servidores SQL de Microsoft cuya cuenta de administrador (SA) tiene contraseña en blanco (configuración por defecto).

El descubrimiento de Frethem y Bugbear (o tanatos) marcan la aparición de malware empaquetados para evitar su detección por parte de los antivirus. El empaquetado consiste en la compresión y encriptación de un archivo ejecutable para disminuir su tamaño y cambiar su apariencia. Estas acciones no necesariamente deben ser utilizadas por programas dañinos aunque suele ser una práctica común.

Otro código malicioso que hisó su aparición es Benjamín, el primer gusano que intenta reproducirse a través de la red de intercambio de archivos formada por los usuarios de la popular aplicación Peer to Peer Kazaa.

En cuanto a Linux aparece Slapper un gusano que intenta aprovecharse de la vulnerabilidad de desbordamiento de buffer en el componente OpenSSL en servidores Apache.

Año 2003

Para este año un concepto antiguo vuelve a sembrar pánico en Internet. El gusano Slammer (Sapphire), utilizando una vulnerabilidad del servidor Microsoft SQL logró record inimaginables de infección.

El gusano Slammer infectó menos computadoras que CodeRed, pero actuó dos veces más rápido infectando más del 90% de las computadoras vulnerables tan sólo 10 minutos después de iniciar su propagación.

Según CAIDA (Cooperative Association for Internet Data Analysis), el Slammer duplicaba su área de su propagación cada 8,5 segundos, y alcanzó 55 millones de equipos rastreados por segundo en 3 minutos, buscando nuevas computadoras vulnerables para infectarlas con el consecuente incremento de tráfico en la red.

En agosto de este año Microsoft comienza su programa de recompensas ofreciendo U$S 250.000 a quien entregue informes sobre creadores de virus.

La segunda epidemia fue causada por el gusano Blaster (o Lovesan o Msblast o Poza), que apareció en agosto aprovechando vulnerabilidades en Remote Procedure Call (RPC) de Windows (corregidas un mes antes) para reproducirse.

El excesivo tráfico que generaba en busca de computadoras vulnerables afectó considerablemente a Internet en los días de su evolución. Contenía una rutina que intentaba conectarse a www.windowsupdate.com en una fecha determinada para ocasionar un ataque DDoS (Distributed Denial of Service o Ataque Distribuido de Denegación de Servicio) y colapsar este servicio de Microsoft.

Con Blaster, por primera vez la recompensas de Microsoft rinden sus frutos, y un joven de 18 años, Jeffrey Parson, admite haber modificado el gusano original y crear una nueva versión del mismo (Blaster.B).

Las formas más comunes para identificarlo eran reinicios inesperados, errores en diversas aplicaciones de Office y, el más común, una ventana informando que el sistema se reiniciará en 60 segundos.

En este año comienzan a conocerse y a utilizarse las botnets (redes zombies). Una botnet es una herramienta que puede ser utilizada con diversos fines (como el conocido proyecto SETI@home para búsqueda de vida extraterrestre), pero que actualmente han logrado su repercusión al ser utilizadas por creadores de malware para difundir sus obras dañinas.

Los fines más comunes de una de estas redes son:

- Distributed Denial-of-Service Attacks (DDoS)
- Distribución de spam y phishing
- Escuchas de tráfico de red (Sniffing)
- Keylogging
- Distribución de nuevos malware
- Abuso de publicidad
- Robo masivo de datos

Los gusanos más conocidos programados para armar estas redes con Agobot (o Gaobot o Morphine o Phatbot o Forbot o XtremBot), RBot (o SDBot o UrBot o UrXBot) y Mydoom/Mytob, existiendo cientos de variantes de ellos y siendo modificados a diario.

El éxito de estos gusanos radica en que son capaces de desactivar el software de seguridad (como firewall y antivirus), explotar diversas vulnerabilidades del sistema para lograr su propagación en decenas de formas e infectar gran variedad de sistemas operativos para lograr los objetivos mencionados.

Según un estudio publicado por www.honeynet.org (organización dedicada al mejoramiento de la seguridad de internet sin costo al público) el tamaño de una botnet es variable y puede llegar hasta 50.000 equipos controlados por un solo grupo.

Año 2004

En enero aparece el destructivo Mydoom, un gusano que se propaga por correo electrónico y la red de intercambio de archivos Kazaa, permitiendo el control remoto del equipo infectado, cuyo objetivo era hacer caer el sitio SCO (corporación desarrolla distribuciones Linux y Unix para servidores y estaciones de trabajo).

El éxito al hacer caer SCO ,demuestra la efectividad de las redes distribuidas (zombies) para realizar ataques de denegación de servicio. Mydoom marcó la historia como el gusano de mayor y más rápida propagación de los últimos tiempos.

En mayo de este año comienza a circular un gusano llamado Sasser, el cual buscaba sistemas Microsoft Windows 2000, 2003 y XP que aún no haya actualizado una vulnerabilidad en el proceso LSASS (Local Security Authority Subsystem).

Comienza a hacerse popular un riesgo mencionado durante años por todos los especialistas en seguridad como es la propagación de código malicioso sobre tecnología móvil.

Así hicieron su aparición creaciones como:

- Cabir, un gusano capaz de reproducirse a través de teléfonos móviles con el sistema operativo EPOC o Symbian (según la versión), aprovechando su posibilidad de conectarse mediante la tecnología inalámbrica Bluetooth.
- Brador, un troyano de origen ruso para dispositivos Pocket PC con el sistema operativo Windows CE. Este troyano es capaz de comunicarse con su autor ,así como de abrir un puerto para que el mismo tome control del equipo infectado.
- Otros ejemplos de este tipo de amenaza móvil son Skull y Mosquito para sistemas Symbian.

Año 2005

Cambia la tendencia de los últimos 5 años, no en cantidad de virus sino los objetivos que buscan los mismos, es así como los gusanos y troyanos se empiezan a encargar de armar

redes de bots para obtener dinero. La idea de “entretenimiento” en la creación de virus ya no es tal, se empezó a convertir en un negocio muy rentable.

La mejor prueba de ello son los denominados espías bankers entre los que se puede contar miles de variantes cuyo principal método de propagación se basa en la modificación permanente de su código y esta forma de evitar la detección de los antivirus.

Estos programas generalmente se distribuyen mediante spam y/o haciendo uso de otros malware.

Estos troyanos roban información relacionada con las transacciones comerciales y bancarias del usuario infectado. Y su forma de funcionamiento es la misma en la mayoría de ellos: el troyano permanece en memoria y monitorea la navegación del usuario y cuando éste accede a sitios webs de instituciones financieras ,captura sus datos sensibles (Nombre de Usuario, Contraseñas, Tarjetas de Crédito, Cuentas Bancarias, etc.).

Entre los gusanos que funcionan como bankers están los de la familia Sober, activos desde octubre del 2003 y se han mantenido en actividad ya que en los principales rankings se los puede ver presentes aun.

Año 2006

La tendencia en este año estuvo orientada a la explotación y utilización de la Ingeniería Social como principal técnica de propagación. También, puede destacarse que la gran mayoría de las amenazas tienen un claro objetivo dirigido a los datos de los usuarios para utilizarlos luego con fines delictivos de distinta índole.

En febrero fue el inicio de los ataques con la aparición de los Bagle, los cuales fueron detectados bajo Win32/Bagle.FA y el Win32/Bagle.EZ, quienes intentaron aprovechar el evento mundial del Súper Tazón de Fútbol Americano para que los usuarios estén distraídos y así se eleve el porcentaje de infección.

Estas amenazas intentan desactivar los distintos programas antivirus y modificar los archivos locales del sistema para que los software de seguridad no puedan ser actualizados.

A inicios de Marzo se unieron a Microsoft Virus Information Alliance (VIA) varios de los más conocidos y grandes proveedores antivirus como ESET, McAfee y Symantec. Los miembros de VIA asisten al equipo de seguridad de servicios de soporte de productos para brindarles a los clientes de Microsoft información detallada acerca de los virus más significativos que puedan afectar a las aplicaciones de Microsoft y a sus clientes.

Debido a la aparición de nuevo malware día a día, es importante que las empresas de antivirus no solo brinden nuevas actualizaciones para identificar estas amenazas una vez que son lanzadas, sino también que sean capaces de detectarlas de manera proactiva a través de la tecnología de heurística avanzada. Ya que sin la detección heurística, los usuarios deben esperar las versiones actualizadas de sus programas antivirus, lo que crea una ventana crítica de vulnerabilidad que puede durar horas, o hasta incluso días.

Aunque ya es un método común del malwere utilizar la Ingeniería Social entre los primeros en utilizarla esta:

Win32/TrojanDownloader.Small.CNK y el Win32/Zippo.10

El Zippo.10 es un troyano que comprime y encripta con clave archivos de acceso común como los .DOC o los .XLS.

Luego, en las carpetas de las cuales obtuvo los archivos originales, crea un archivo explicando al usuario como debe proceder para recuperar los archivos en cuestión. En este caso, se debería abonar 300 dólares como “rescate” para recuperarlos.

Constantemente aparecen nuevos mensajes que hacen uso de la Ingeniería Social e intentan engañar a los usuarios, por lo que es muy importante controlar los mensajes recibidos ya que el “modelo” de infección basado en la Ingeniería Social y en el cobro por la recuperación de archivos es un negocio muy importante para fines delictivos. Entre los

ejemplos principalmente utilizados están mensajes relacionados a los famosos de cualquier índole, así como también, prestar más atención con sucesos mundiales, noticias de farándula o la más utilizada publicitando fotos o información de famosos.

En mayo de este año hacen aparición sitios que ofrecen un supuesto servicio gratuito al usuario. Los mismos van desde instalar algún software para limpiar nuestra computadora de un supuesto virus o amenaza.

Su forma de funcionamiento es que cuando el usuario acepta el servicio propuesto, el sitio web procede a instalar un software el cual atentan contra la seguridad del sistema infectado y la privacidad del usuario.

Si bien la existencia de esto sitios es ampliamente conocidas por las empresas antimalware, la detección de los mismos se torna difícil debido a la cantidad y velocidad en que aparecen los mismos.

En octubre aparece el troyano bancario Win32/Bancodor.AB. Los troyanos bancarios afectan principalmente a América Latina.

El funcionamiento de los troyanos bancarios es muy similar, ya que todos poseen el mismo objetivo: obtener los datos personales de instituciones financieras para robar el dinero de los usuarios infectados. Aunque hay que destacar que cada día son más efectivas y novedosas las técnicas utilizadas, como es el caso de los nuevos troyanos que capturan videos o imágenes para vulnerar la utilización de los teclados virtuales.

Año 2007

Como práctica común el malware toma como ventaja para infectar sistemas las fechas festivas es así como en el 1ro de Enero la epidemia del Win32/Nuwar.M. un gusano de correo electrónico que fue detectado con altos niveles de propagación durante los primeros días de año 2007.

Nuwar.M llegaba a los usuarios como un mensaje de felices fiestas, con un archivo adjunto que normalmente se llama postcard.exe que al ser ejecutado trata de continuar propagándose y descargar componentes de internet.

El malware utiliza a gusanos, troyanos y otras tantas amenazas informáticas, los cuales son propagados mediante mensajes los cuales parecen ser saludos o tarjetas virtuales, las que son enviadas posteriormente a través de cientos de miles de mensajes de correo electrónico, los mensajes contienen archivos adjuntos del tipo postcard.exe o con enlaces a páginas de tarjetas virtuales falsas. Estos mensajes pueden engañan a los usuarios al retornar a las actividades normales tras las fiestas y estar mezclados en su bandeja de entrada con saludos reales como por ejemplo de navidad o de fin de año.

En Marzo el phishing se masifico en Centro América, el país más afectado fue Panamá, debido a la cantidad de importantes Instituciones Financieras que funcionan en ese país.

El phishing es una de las amenazas más peligrosas de la actualidad por su el riesgo que implica que la víctima pierda dinero. Es conformado de mensajes de correo electrónico falsificados con la intención de engañar a usuarios crédulos, para que revelen sus números de tarjetas de crédito, den información de sus depósitos de cuentas bancarias y todo tipo de detalles personales.

Por este motivo, los usuarios que caen en esta trampa pueden recibir daños mucho mayores que inconvenientes con la computadora, como es la pérdida total o parcial de su dinero en la cuenta bancaria o la tarjeta de crédito, dependiendo de cada caso.

En Agosto nuevamente un troyano por medio de un mensaje de Ingeniería Social que se aprovecha de la confianza y popularidad de Google, que simula ser una Alerta del servicio News Google y descarga un troyano cuando se intenta ingresar en algún enlace del correo.

News.Google.com es un servicio de la empresa Google que provee noticias a nivel mundial de muchas fuentes de información en distintos idiomas y sus usuarios tienen la posibilidad de recibir alertas del sistema según palabras específicas que ellos soliciten.

Este nuevo mensaje engañaba a los usuarios desprevenidos que al hacer clic en alguno de los enlaces del mensaje eran infectados por el troyano:

Win32/TrojanDownloader.Psyme.HX.

El mensaje malicioso era enviado masivamente y en apariencia era completamente igual al enviado por News Google y eso genero la confusión de los usuarios que fueron infectados.

En Septiembre se detecta a un troyano creador de botnets propagándose activamente a través de mensajería Instantánea MSN que se está propagando masivamente en distintos países de Iberoamérica que enviaba con mensajes en español, portugués y también en inglés.

El troyano SdBot una vez infectado el equipo, toma control del mismo transformándolo en una PC zombi que forma parte de una botnet las cuales tienen como principal objetivo agregar nuevos equipos a sus redes botnet para luego utilizarlas en beneficios propio según les convenga. SdBot aprovecha la conexión de los usuarios al MSN para enviarse a sí mismo a todos los contactos del equipo infectado. Esto lo hace mediante múltiples mensajes.

El mensaje invita al usuario a aceptar el archivo enviado a través de distintas frases como:

> "jajajaja recuerda cuando tuviste el pelo así" o "Esta es la foto nuestra que voy a poner en MySpace"; como posibles mensajes en castellano, mientras que en inglés podría ser "Wanna see the pics from my vacation".

El archivo enviado por el equipo infectado tiene siempre el mismo nombre base: IMG-0012, aunque también en algunos casos se envía como IMG-0012[texto variable]. Este archivo siempre está comprimido en formato .zip o .rar, y es el que contiene al troyano Win32/SdBot el cual tiene exactamente el mismo nombre que el archivo comprimido y es de extensión .com.

Año 2008

Para Enero se advierte acerca del uso de perfiles falsos de MySpace para propagar malware. Cuando se ingresa al perfil falso de un usuario de MySpace creyendo que es el legítimo, en realidad se está ingresando a otro sitio web que simula ser el real y contiene un troyano downloader que luego descargará otros códigos maliciosos.

Los falsos perfiles de MySpace prácticamente son iguales visualmente a los originales y además, poseen una dirección web muy similar a la real. De esta manera, se aumenta la efectividad del engaño posibilitando que más usuarios puedan ser víctimas de este ataque. Esta técnica utilizada es muy similar a la del phishing en torno a la simulación de un sitio web real a través de una página web falsa y maliciosa aunque en este caso la intención de los perfiles falsos de MySpace es únicamente la descarga de malware.

Para fines de Enero se advierte un aumento significativo de malware que se propaga a través de diversos medios externos entre el más conocido las memorias USB, el malware conocido como INF/Autorun quien encabezo los ranking de detecciones.

Entre los virus maliciosos que se trasmiten por los dispositivos los más conocidos son:

1. **INF/Autorun:** Utilizado para ejecutar y proponer acciones automáticamente cuando un medio externo como un CD, un DVD o un dispositivo USB, es leído por el equipo informático.
2. **Win32/Pacex.Gen:** Código malicioso que genera archivos los cuales se utilizan para el robo de contraseñas.
3. **Win32/Adware.Virtumonde:** Es un adware con propiedades de spyware utilizado para enviar publicidad a los usuarios infectados.
4. **Win32/Obfuscated.A1:** Archivos que utilizan técnicas sospechosas para evadir la detección de antivirus. Incluyen la instalación de paquetes adware como el Virtumonde.
5. **Win32/Adware.Virtumonde.FP:** Un adware que durante su ejecución, despliega ventanas emergentes con diferentes tipos de publicidad.

6. **Win32/Adware.Ezula:** Es un adware que se instala silenciosamente y sin proporcionar información al usuario acerca de lo que podría estar instalando en el sistema. Además de descargar y ejecutar software adicional, esporádicamente exhibe publicidades durante la navegación por Internet.

7. **Win32/TrojanDownloader.Ani.Gen:** Es una amenaza que aprovecha una vulnerabilidad (corregida por Microsoft) en los archivos .ANI (utilizados para contar con cursores e íconos animados en Windows) para descargar malware como troyanos, gusanos o secuestradores de contraseñas.

En Junio se advirtió el envío masivo de correos electrónicos maliciosos aprovechando Facebook y Hi5. Al igual que en cualquier caso tradicional de phishing el usuario recibe un correo electrónico que simula ser una invitación a la red social en cuestión con enlaces hacia el supuesto sitio web ingresará a un sitio idéntico al real pero falso en el que se piden usuarios y contraseñas.

Si el usuario completa el formulario con sus datos personales, automáticamente serán enviados al atacante para que los pueda utilizar en forma fraudulenta para su conveniencia.

El objetivo de este ataque es conseguir información personal de la víctima, así como también robar el perfil en la red social y datos privados de los contactos, los cuales podrían ser utilizados maliciosamente de distintas maneras como por ejemplo tomar la información personal del perfil robado y sus contactos para hacer ataques de spam, phishing o malware dirigidos con datos reales para generar confianza en la posible nueva víctima.

Agosto también reporto gran aparición de los rogue son falsos programas de seguridad que bajo el pretexto de ser gratuitos intentan lograr ser instalados, para luego solicitar la registración económica del mismo el robo de información privada del usuario y la posterior instalación de adware y spyware.

El rogue Antivirus XP 2008 fue la principal amenaza propagada durante este mes debido a la gran cantidad de técnicas utilizadas para llegar al usuario y por la diversidad de metodologías de Ingeniería Social utilizadas para engañarlo e infectarlo.

En Octubre tras la aparición de un nuevo gusano de Internet demuestra la importancia de las actualizaciones del sistema ya que el nuevo gusano que aprovecha la vulnerabilidad crítica de los sistemas operativos Windows 2000, XP, 2003, 2008 y Vista.

La vulnerabilidad afecta al protocolo RPC y permite la ejecución de código remoto en el equipo del usuario sin interacción ni autenticación del mismo. El gusano se llama Win32/Gimmiv.

El gusano Gimmiv tiene como objetivo dar acceso al sistema infectado al creador del malware enviando información sobre cualquier información relevante del usuario como podría ser:

- Usuarios y contraseñas de distintos sistemas instalados en el equipo
- Contraseñas almacenadas en el navegador y el cliente de correo, como podrían ser sobre cuentas bancarias, correos electrónicos y/ otros servicios
- Cookies y otros medios de autenticación
- Cualquier archivo del sistema que pueda ser considerado relevante por el atacante

De esta forma, se puede ver claramente la importancia de siempre contar con un sistema operativo y sus aplicaciones actualizados constantemente, además de optar por una solución antivirus con capacidades de detección proactiva con la posibilidad de descubrir código maliciosos conocidos y desconocidos.

Año 2009

Durante enero se observó una oleada de infecciones en millones de equipos alrededor del mundo a través del Conficker es un gusano que utiliza viejas técnicas de engaño y se aprovecha de vulnerabilidades en sistemas no actualizados. Este gusano aprovecha una vulnerabilidad crítica de Windows, que ya fue resuelta por Microsoft, pero las versiones

posteriores del Conficker comenzaron a utilizar otros medios tales como los recursos compartidos de los equipos y el archivo autorun.ini de los dispositivos de almacenamiento removibles para garantizar nuevas vías de propagación de esta amenaza.

Durante Marzo Conficker se mantuvo como uno de los códigos maliciosos de mayor propagación, destacándose por sus elevados índices de infección.

Pero contrario a la curva frecuente de infección, donde el número de sistemas infectados suele disminuir con el pasar del tiempo la constante aparición de nuevas variantes del Conficker hiso de este gusano una de las amenazas más complejas de la actualidad debido a la creciente cantidad de usuarios afectados junto con un incremento acelerado en sus niveles de propagación alrededor del mundo.

La aparición del gusano Conficker se remonta a noviembre del año 2008 fecha en la que comenzó la propagación de su primera variante aprovechando una vulnerabilidad en los sistemas operativos Windows. El gusano se aprovecha de un problema ya solucionado (Parche MS08-067), pero debido a que aún existe una gran cantidad de usuarios que no han instalado dicha actualización, la amenaza continúa propagándose por este medio.

Su forma de contagio y funcionamiento son:

- Como foco de contagio la utilización los recursos compartidos o los dispositivos USB
- Y en su funcionamiento la elevación y saturación del tráfico en la red causando denegaciones de servicio y posible fuga de información crítica entre otros inconvenientes. Todo ello, sin considerar los costos humanos, de tiempo y económicos requeridos para eliminar el gusano.

Koobface fue el malware que más se dispersó en Twitter, al contagiarse con el gusano el usuario infectado y conectado a la red social automáticamente se enviarían mensajes a todos sus contactos con el mensaje:

> “My home video :)” y una dirección web acortada.

Si el usuario ingresa a dicha dirección, se abrirá una página simulando un supuesto video y se intentará descargar un archivo ejecutable que resulta ser esta nueva variante del gusano.

Tabla Resumen 1: Historia del Malware	
Génesis 1800 a 1960	• George Boole describió su algebra que dio origen a la ciencia de la computación. • Claude Elwood Shannon estableció el paralelismo entre la lógica de Boole y los circuitos de lógicos. • Los premios Nobel John Bardee, Walter Brattain y William B. Shockley diseñan el transistor en 1947. • El premio Nobel Jack S. Kilby (Texas Instruments), desarrolla el microchip, en 1959. • IBM establece un estándar con su primer PC con el sistema operativo PC-DOS, En 1981.
Prehistoria 1948 - 1983	• En los laboratorios de Bell Computer, Robert Thomas Morris, Douglas McIlroy y Victor Vysottsky crean un juego CoreWar. o Donde programas combaten entre sí con el objetivo de ocupar toda la memoria de la máquina eliminando y así terminando con los oponentes. • Nace Creeper en 1972 desarrollado por Robert Thomas Morris. Emitía el mensaje: "I´m a creeper… catch me if you can!" periódicamente. o Para su eliminación se creó otro virus llamado Reaper programado para buscarlo y eliminarlo. Dando paso a los primeros intentos de creación de un antivirus. • En 1975, John Walker (fundador de Autodesk), descubre una forma de distribuir un juego dando origen al primer troyano de la historia. El "Animal/Pervade". o **Animal:** Software que pedía al usuario adivinar el nombre de un animal en base a preguntas realizadas. o **Pervade:** Rutina capaz de actualizar las copias de Animal en los directorios de los usuarios cada vez que el mismo era ejecutado, de allí que sea un troyano.
Década de los 80's	• En 1981, Richard Skrenta escribe el primer virus de amplia reproducción el Elk Cloner que se almacena en el sector de inicio de los disquetes de 360 kb capaz de residir en memoria luego que el disco era retirado (Mostraba una leyenda a los 50 reinicios). • En 1984, Frederick B. Cohen publica sus estudios "Computer Viruses - Theory and Experiments", donde define por primera vez a los virus. Definición propuesta y aceptada por la comunidad es: "Programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí mismo" • Por ser el precursor del estudio de los códigos maliciosos ,Cohen es

	conocido como el “Padre de los virus” aunque no fue el primero en trabajar sobre ellos. • En el año de 1988, Leonard Adleman en su artículo “An Abstract Theory of Computer Viruses” introduce los conceptos de cuarentena, desinfección, infección y el término Troyano. • En 1987, apareció el primer virus capaz de infectar Macintosh el MacMag. Distribuido a través de disquetes entregados a los miembros del Club Mac. Se limitaba a presentar un mensaje de paz en pantalla y al llegar el 2 de Marzo de 1988 (aniversario del Macintosh II), se auto eliminaba.
Década de los 90's	• Se funda EICAR en Hamburgo, Alemania. Este instituto es el autor del archivo “EICAR” con la finalidad de probar la eficacia de un antivirus sin involucrar el riesgo de trabajar con un virus real. • En 1991, se crea CARO el cual planteo técnicas para nombrar a los virus. CARO decide que los virus deben bautizarse de la siguiente manera: Family_Name.Group_Name.Major_Variant.Minor_Variant[Modifier] (Prefijo.Nombre.Variante) • En 1993, el experto en antivirus Joe Wells crea una lista con 104 virus denominada WildList. Actualmente esta lista cuenta con la participación de 80 investigadores de todo el mundo. • Microsoft lanza su propio antivirus: Microsoft AntiVirus (MSAV), basado en Central Point AntiVirus (CPAV). • Con Windows 95 aparecen nuevos conceptos de infección, así Sarah Gordon descubre Concept, mismo que infectó a miles de documentos de Microsoft Word. o Concept es el primer virus de macro escrito en el lenguaje WordBasic capaz de infectar cualquier plataforma que ejecutara MSWord (PC y Mac). • En 1997 se crea el virus CIH creado por un taiwanés (iniciales de su autor, Chen Ing-Hou) o Chernovyl. Su rutina borraba los primeros 2048 sectores del disco rígido y sobrescribía algunos tipos de Flash-Bios dejando inutilizable la placa madre de la computadora. • Para marzo de 1999 Melissa comenzó a llegar a miles de correos en un archivo adjunto el cual aparecía enviado por un contacto conocido. Este virus fue el encargado de desechar la idea de que es una buena práctica de seguridad: “no abrir mensajes de personas desconocidas”, ya que el virus se adjuntaba en correos de contactos de confianza.

Tabla 1: Tabla de resumen historia del Malware desde el génesis hasta la década de los 90’s.
Fuente: Hugo Paredes. **Fecha elaboración:** Enero 2010.

Tabla Resumen: Historia del Malware Década Actual	
2000	• En el 2000 el popular un generador de gusanos VBSWG (Visual Basic Script Worm Generator) genero uno de los mejores ejemplos de virus creados por software el virus bautizado Anna Kournikova, que incluso llegó a infectar a la NASA. • Otra creación de ese año fue el “gusano del amor” :LoveLetter. El cual llegaba por correo con un adjunto y su nombre se debe a que el asunto del mensaje era “ILOVEYOU”.
2001	• En el mes de julio aparece CodeRed se propaga buscando servidores con IIS 5.0 vulnerables. El gusano ingresa al sistema a través del puerto 80 explotando una vulnerabilidad ya corregida. El gusano continuó su expansión debido a la irresponsabilidad de los administradores y no utilizar la respectiva actualización. • CodeRed logró infectar 80.000 servidores en las primeras horas de la fecha de su ataque y llegó a duplicar su área de propagación cada 37 minutos. • En mayo aparece un nuevo tipo de ataque sin utilizar código malicioso el bautizado hoax (mensaje de correo de correo electrónico) en el que se alerta acerca que un programa (sulfnbk.exe) es un peligroso virus. o El mensaje daba instrucciones para eliminar este archivo si era hallado. Pero el archivo efectivamente siempre es encontrado porque pertenece a Windows. Al eliminarse algunas capacidades del sistema operativo dejaban de funcionar.
2002	• En enero de este año aparece el primer virus capaz de infectar Macromedia Shockwave Flash (archivos .SWF) y programado en ActionScript. • En mayo el gusano Spida comienza a aprovecharse de servidores SQL de Microsoft cuya cuenta de administrador (SA) tiene contraseña en blanco (configuración por defecto). • El descubrimiento de Frethem y Bugbear marcan la aparición de malware empaquetados (zip o rar) para evitar su detección por parte de los antivirus ya que cambian su apariencia.
2003	• En agosto de este año Microsoft comienza su programa de recompensas ofreciendo U$S 250.000 a quien entregue informes sobre creadores de virus. o Así con Blaster, por primera vez la recompensas de Microsoft rinden sus frutos, y un joven de 18 años, Jeffrey Parson, admite haber modificado el gusano original y crear una nueva versión del mismo (Blaster.B). • Blaster apareció en agosto aprovechando vulnerabilidades en Remote Procedure Call (RPC) de Windows. Contenía una rutina que intentaba conectarse a www.windowsupdate.com en una fecha determinada para

	ocasionar un ataque DDoS y colapsar este servicio de Microsoft. • En este año comienzan a conocerse y a utilizarse las botnets (como el proyecto SETI@home de búsqueda de vida extraterrestre) pero actualmente son utilizadas por creadores de malware para difundir sus obras dañinas. Los fines más comunes de una de estas redes son: DDoS, distribución de spam y phishing, Sniffing, Keylogging, Abuso de publicidad, Robo masivo de datos, etc. • Según el estudio publicado por www.honeynet.org (organización dedicada al mejoramiento de la seguridad de internet sin costo al público) el tamaño de una botnet es variable y puede llegar hasta 50.000 equipos controlados por un solo grupo.
2004	• En enero aparece Mydoom gusano que se propaga por correo electrónico y la red de intercambio de archivos como Kazaa, permitiendo el control remoto del equipo infectado cuyo objetivo era hacer caer el sitio SCO (corporación que desarrolla distribuciones Linux y Unix para servidores y estaciones de trabajo). • Mydoom demuestro la efectividad de las redes distribuidas (zombies) para realizar ataques de denegación de servicio. Mydoom es el gusano de mayor y más rápida propagación de los últimos tiempos. • En mayo de este año comienza a circular un gusano llamado Sasser, el cual buscaba sistemas Microsoft Windows 2000, 2003 y XP que aún no haya actualizado una vulnerabilidad en el proceso LSASS (Local Security Authority Subsystem). • Comienza a hacerse popular un riesgo mencionado durante años por todos los especialistas en seguridad como es la propagación de código malicioso sobre tecnología móvil. Con aparición de creaciones como: ○ Cabir gusano capaz de reproducirse a través de teléfonos móviles con el sistema operativo EPOC o Symbian aprovechando su posibilidad de conectarse mediante Bluetooth. ○ Brador, un troyano de origen ruso para dispositivos Pocket PC con el sistema operativo Windows CE. Capaz de comunicarse con su autor permitiendo tomar el control del equipo infectado. ○ Otros ejemplos de este tipo de amenaza móvil son Skull y Mosquito para sistemas Symbian.
2005	• Se detectan espías conocidos como bankers su propagación se basa en la modificación permanente de su código y esta forma de evitar la detección de los antivirus. • Estos troyanos roban información relacionada con las transacciones comerciales y bancarias del usuario infectado. ○ Funciona como la mayoría de los troyano permanece en memoria y monitoreando la navegación del usuario así cuando éste accede a sitios webs de instituciones financieras ,captura sus datos sensibles (Nombre de Usuario, Contraseñas, Tarjetas de Crédito, Cuentas

	Bancarias, etc).
2006	• La tendencia en este año estuvo orientada a la explotación y utilización de la Ingeniería Social como principal técnica de propagación. • En Marzo se crea en conjunto con Microsoft la Virus Information Alliance (VIA) con los más grandes proveedores antivirus como ESET, McAfee y Symantec. Los miembros de VIA brindan a clientes de Microsoft información detallada acerca de los virus más significativos que puedan afectar a las aplicaciones de Microsoft. • Aunque ya es un método común del malware utilizar la Ingeniería Social entre los primeros en utilizarla está el: o El Zippo.10 es un troyano que comprime y en cripta con clave archivos de acceso común como los .DOC o los .XLS. o Luego, en las carpetas de las cuales obtuvo los archivos originales, crea un archivo explicando al usuario como debe proceder para recuperar los archivos en cuestión. En este caso, se debería abonar 300 dólares como "rescate" para recuperarlos. • En mayo de este año hacen aparición sitios que ofrecen un supuesto servicio gratuito al usuario. Los mismos van desde instalar algún software para limpiar nuestra computadora de un supuesto virus o amenaza.
2007	• Como práctica común el malware toma como ventaja para infectar sistemas las fechas festivas es así como en el 1ro de Enero la epidemia del Win32/Nuwar.M. un gusano de correo electrónico que fue detectado con altos niveles de propagación durante los primeros días de año 2007. • En Septiembre se detecta a un troyano creador de botnets propagándose activamente a través de mensajería Instantánea MSN que se está propagando masivamente en distintos países de Iberoamérica que enviaba con mensajes en español, portugués y también en inglés. o El mensaje invita al usuario a aceptar el archivo enviado a través de distintas frases como: o "jajajaja recuerda cuando tuviste el pelo así" o "Esta es la foto nuestra que voy a poner en MySpace"; como posibles mensajes en castellano, mientras que en inglés podría ser "Wanna see the pics from my vacation".
2008	• Para Enero se advierte acerca del uso de perfiles falsos de MySpace para propagar malware. Cuando se ingresa al perfil falso de un usuario de MySpace creyendo que es el legítimo, en realidad se está ingresando a otro sitio web que simula ser el real y contiene un troyano downloader que luego descargará otros códigos maliciosos. • Para fines de Enero se advierte un aumento significativo de malware que se propaga a través de diversos medios externos entre el más conocido las memorias USB, el malware conocido como INF/Autorun quien encabezo los ranking de detecciones.

	• En Junio se advirtió el envío masivo de correos electrónicos maliciosos aprovechando Facebook y Hi5. Al igual que en cualquier caso tradicional de phishing el usuario recibe un correo electrónico que simula ser una invitación a la red social en cuestión con enlaces hacia el supuesto sitio web ingresará a un sitio idéntico al real pero falso en el que se piden usuarios y contraseñas.
2009	• Durante enero se observó una oleada de infecciones en millones de equipos alrededor del mundo a través del Conficker es un gusano que utiliza viejas técnicas de engaño y se aprovecha de vulnerabilidades en sistemas no actualizados. • El gusano se aprovecha de un problema ya solucionado (Parche MS08-067), pero debido a que aún existe una gran cantidad de usuarios que no han instalado dicha actualización, la amenaza continúa propagándose por este medio. • Su forma de contagio y funcionamiento son: ○ Como foco de contagio la utilización los recursos compartidos o los dispositivos USB ○ Y en su funcionamiento la elevación y saturación del tráfico en la red causando denegaciones de servicio y posible fuga de información crítica entre otros inconvenientes. Todo ello, sin considerar los costos humanos, de tiempo y económicos requeridos para eliminar el gusano.

Tabla 2: Tabla de resumen historia del Malware década actual.
Fuente: Hugo Paredes. **Fecha elaboración:** Enero 2010.

Aunque existen gran variedad de tecnologías y sistemas, muchos de los cuales son compatibles entre sí, no han impedido que las distintas amenazas se propaguen y tengan éxito. Algo que ha enseñado la historia es que solo son obstáculos en el camino para los desarrolladores de malware, los cuales irán descifrando con ayuda de los avances en la tecnología y facilidad de comunicación que existe ahora entre los distintos dispositivos electrónicos que utilizamos diariamente.

Debido a la gran cantidad código malicioso generando año tras año mismo que ya no solo causa daños al sistema operativo sino también que también apunta robo de información sensible con fines fraudulentos se han ido creando organizaciones como **http://www.honeynet.org/about** y asociaciones entre las principales empresas de software de seguridad como **Microsoft Virus Information Alliance (VIA)**, para detectar amenazas las crecientes amenazas de spyware, adware, phissing, etc.

Así es como esta mutua colaboración y desarrollo ha perfeccionado las técnicas para la detección de código malicioso, minimizado el tiempo entre la publicación de un nuevo código malicioso y la posterior corrección de las vulnerabilidades que ataca, ahora en apenas horas se publica la solución. Ya que con anteriores ejemplos tomaron cantidades considerables de tiempo como:

CodeRed año 2001 28 días

Blaster/Lovsan año 2003 26 días

Sasser año 2004 17 días

Zotob año 2005 4 días

Esto pone en evidencia que a medida que transcurre el tiempo al aparecer un nuevo código malicioso la detección y solución disminuye.

Aunque actualmente la plataforma más ampliamente utilizada es Microsoft Windows sobre 32 bits. No se debe dejar de pensar que otros sistemas operativos como MAC OS, Linux,

BSD, etc. Pueden estar exentos de amenazas ya que es fácil de predecir que serán blanco de mayores ataques siempre las distribuciones más utilizadas por los usuarios finales.

No se debe dejar de lado que los creadores de malware apuntaran sus conocimientos al código multiplataforma que gracias a la cantidad de tecnología disponible como PDAs, wi-fi, SMS, MMS, software de 32-64 bits y múltiples sistemas operativos; son sólo algunos de los lugares donde, sin duda, el malware terminará haciendo escala. Pero vale la pena recalcar que la responsabilidad de mantener la seguridad en nuestros sistemas ya no solo recae en los administradores de red, sino que también de los usuarios, quienes deben capacitarse en nociones básicas de seguridad en el uso de sus sistemas ya que ataques como los de Ingeniería Social no dependen solo del software o políticas implantadas al sistema operativo sino también de la capacidad del usuario para detectar posibles ataques de código malicioso y aprender que la seguridad en un sistema no se encuentra en estado estático sino que también varía muy rápido al pasar del tiempo.

1.3 Clasificación del Malware

Debido a la cantidad de variaciones que el malware tubo a través de los años los expertos han realizado una clasificación para indicar cuáles son sus respectivos funcionamientos y como afectan a los sistemas, aunque con el tiempo los ataques se han ido tecnificando llegando hasta ataques que utilizan ya no solo ingeniería técnica sino también social y se los ha clasificado en:

- Virus Informático y su descripción.
- Virus ejecutables.
- Virus residentes en memoria.
- Virus de sector de arranque.
- Macro Virus.
- Virus de Correo Electrónico.
- Gusano.
- Troyano.
- Exploits.
- Rootkits.
- Backdoors.

- Redes de Bots (BotNet).
- Keyloggers.
- Ransomware.
- Spam.
- Hoax.
- Scam.
- Phishing.
- Spyware.
- Adware.
- Ingeniería Social.

1.3.1 Virus Informático

Su nombre proviene del latín "veneno" y de su semejanza con los virus biológicos ya que su forma de actuar es similar:

- Ambos utilizan a un huésped (PC) e inician sus actividades en forma imperceptible hasta que se manifiestan los síntomas.
- Los dos hacen uso del huésped para seguir su desarrollo.
- Ambos tienen como objetivo reproducirse y modificar el normal comportamiento del huésped.

Debido a esto se considera a un Virus Informático (VI) como un archivo, porción de código o programa de software ejecutable capaz de reproducirse, auto-ejecutarse, propagarse y ocultarse.

1.3.2 Descripción de un virus

Los virus informáticos no son más que programas diseñados para modificar a otro programa con el objetivo de propagarse. Así su funcionamiento se lo puede relacionar con la gráfica mostrada a continuación:

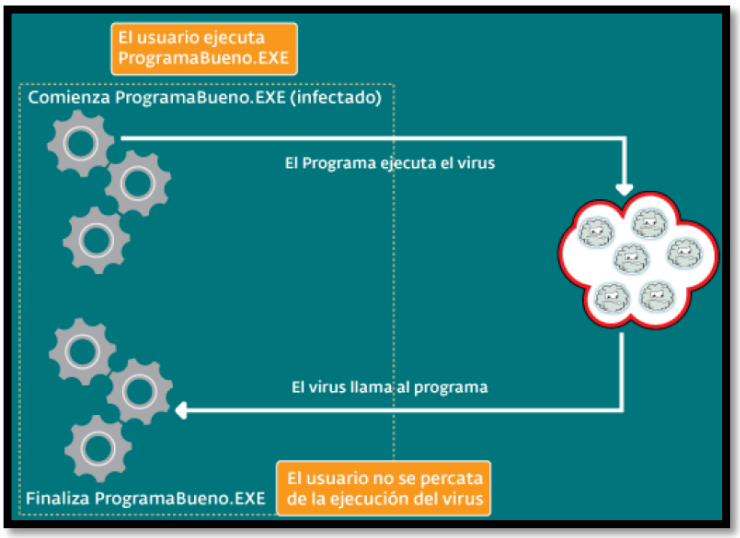


Figura 1: Modelo de Virus. Curso de seguridad informática ESET.
Fuente: http://www.eset-la.com/centro-amenazas/educacion.php

En la gráfica se muestra de forma general el comportamiento básico de un Virus, así cuando el usuario ejecuta el "programabueno.exe" donde está contenido el virus, el código del mismo se ejecuta y toma control por un breve periodo de tiempo en el cual realiza las acciones para las que fue programado y devuelve el control al huésped (PC) y como es común en estos casos, para el usuario fueron imperceptibles las acciones realizadas por el virus.

1.3.3 Virus Ejecutables

Este tipo de virus son los más comunes debido a que atacan a los programas ejecutables con extensiones como (.exe, .com, .dll, .sys, .pif) que son las más utilizadas por el PC y por esta razón logran expandirse en gran medida.

Su forma de funcionamiento es unirse al programa del huésped (PC) mediante diversas técnicas una vez que se pone en marcha el programa ejecutable lo hace también el virus por primera vez y es cuando este queda residiendo en la memoria del PC buscando otros archivos de tipo ejecutable para realizar el mismo ciclo de infección.

Figura 2: Virus Ejecutables. Curso de seguridad informática ESET.
Fuente: http://www.eset-la.com/centro-amenazas/educacion.php

1.3.4 Virus residentes en memoria

Este tipo de virus al residir en la memoria pueden tomar el control de las acciones realizadas por el sistema operativo o el usuario, así cada vez que se accede a un tipo de archivo que el virus sea capaz de infectar, de acuerdo a su programación, procederá a infectarlo tomando en cuenta que el usuario debió haber recibido o ejecutado previamente un archivo infectado.

1.3.5 Virus de sector de arranque

Este tipo de virus es el de mayor perjuicio para el sistema operativo por que residen en los primeros 512 Bytes del disco duro donde se encuentra el sector de arranque o buteo. Estos virus aprovechan este espacio del disco para ejecutar el código que contienen asegurándose que cada vez que arranca el sistema automáticamente se ejecuta e infecta el sistema y para poder solucionar este tipo de problemas se requiere de personal calificado.

Otra acción que también pueden realizar es almacenar el sector de arranque original en otro sector del disco de forma tal que posterior a su ejecución pueden restaurar el sector de arranque para que el sistema se pueda volver a ejecutar.

1.3.6 Macrovirus

Debido a la capacidad que tienen las aplicaciones de ofimática (Microsoft Office y OpenOffice) de ejecutar macros los cuales incluyen programación para realizar alguna

función. Los virus también pueden explotar esta funcionalidad para incluirse y ejecutar su código mediante la misma.

Su forma de infección es mediante la ejecución de un archivo infectado así cada vez que se genera un documento nuevo o se modifique, éste ya contendrá el macrovirus porque la aplicación ya fue infectada por el mismo.

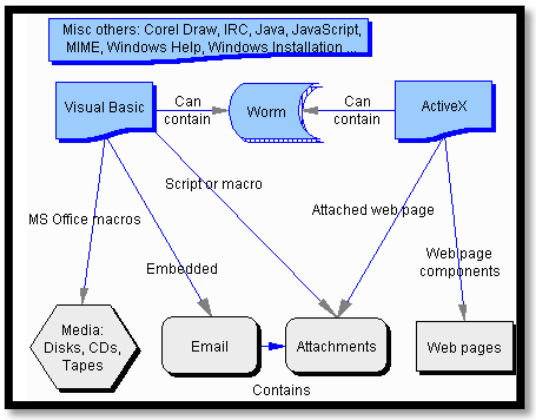


Figura 3: Macro Virus.
Fuente: http://www.livinginternet.com/i/is_vir_mac.htm

1.3.7 Virus de correo electrónico

Debido a la masificación de acceso a este tipo de comunicación en los últimos años se ha convertido en uno de los principales focos de infección. Aunque este tipo de virus explotan diferentes técnicas de Ingeniería Social, siempre manejan un esquema común de propagación:

- Un usuario recibe un correo con un virus.
- Abre el correo y el virus se ejecuta infectando su computadora.
- El virus es capaz de auto-enviarse a los contactos y seguir la cadena de reproducción.

Los virus explotan de forma masiva este medio por su facilidad de llegar a cualquier parte del mundo en donde un PC posea una conexión a internet o correo electrónico.

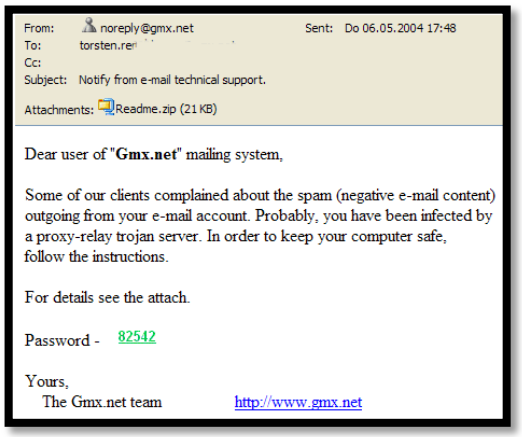


Figura 4: Virus de correo electrónico.
Fuente: http://www.rendelmann.info/blog/default,date,2004-05-07.aspx

1.3.8 Gusano

Son desarrollados para reproducirse por algún medio de comunicación como el correo electrónico o las redes P2P. Y su principal objetivo es llegar a la mayor cantidad de usuarios posibles y lograr distribuir otro tipo de códigos maliciosos. Los cuales tienen diversos fines como engaño, robo o estafa. Entre sus principales funcionalidades también está el de realizar ataques de Denegación de Servicio Distribuido (DDos) contra sitios webs específicos (Windows Update).

Figura 5: Gusano Bangle el cual llega por correo. Donde puede preciarse el archivo adjunto se llama “Margrett.zip”. Curso de seguridad informática ESET.
Fuente: http://www.eset-la.com/centro-amenazas/educacion.php

Figura 6: Gusano Bangle contenido del archivo adjunto. Curso de seguridad informática ESET.
Fuente: http://www.eset-la.com/centro-amenazas/educacion.php

1.3.9 Troyano

Su nombre se deriva con la similitud que tiene con el "caballo de Troya" utilizado por los griegos.

Es un programa generalmente incluido en otra aplicación de utilidad para el usuario. Este código malicioso se ejecuta a la vez con la aplicación donde fue alojado permitiéndole acceso al sistema evitando la autentificación de seguridad en el Sistema Operativo.

Aunque no es denominado como un virus ya que no cumple con todas las características del mismo pero en vista que utiliza otras aplicaciones para diseminarse en forma fraudulenta es catalogado como amenaza.

El principal objetivo de un troyano es pasar inadvertido al usuario después de instalarse y en la actualidad es utilizado para diseminar otro tipo de malware, el cual le permita al creador del troyano acceso a información del Sistema. Otra práctica común es simular que realiza una función útil para el usuario y así tienen campo abierto para acciones dañinas.

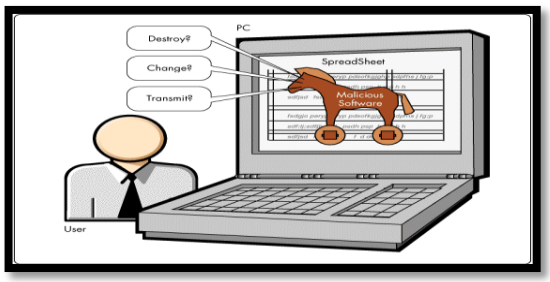


Figura 7: Troyano o caballo de Troya.
Fuente: http://support.novell.com/techcenter/articles/ana19971101.html

1.3.10 Exploits

Su nombre se deriva de su comportamiento, ya que es un programa o código que "explota " vulnerabilidades existentes en el Sistema Operativo. Aunque no es en sí un código malicioso, es utilizado generalmente como un componente de otro tipo de malware para permitir acceso al Sistema y permitirle utilizar funciones que por defecto se encuentran limitadas o controladas en acceso a usuarios administradores. Dependiendo de la vulnerabilidad del sistema se crea uno o varios Exploit para explotarla.

1.3.11 Rootkits

El termino derivo de los sistemas Unix porque es utilizado por diferentes utilidades y herramientas que permiten acceso del administrador al sistema con el uso del comando ("root").

El término evoluciono con el paso del tiempo y ahora es conocido como el conjunto de herramientas utilizadas en cualquier sistema para permitir el acceso fraudulento al mismo. Este tipo de malware generalmente trabaja de forma transparente al usuario ya que permiten acceso al sistema e incluso tomar control del mismo.

Aunque existen actualmente programas debidamente controlados utilizados por las empresas u organizaciones que sirven para dar soporte de TI, controlar ciertos componentes del PC o para denegar acceso a los mismos. Se debe recordar que estos programas deber ser utilizados con ética profesional y es muy importante mantener esto presente ya que el uso inadecuado es éticamente incorrecto y en muchos casos ilegal.

1.3.12 Backdoors

Como se entiende con su traducción al español son programas diseñados para abrir “puertas traseras” en nuestros sistemas como por ejemplo puertos de comunicación que por

defecto esta cerrados, de tal modo que permiten a los creadores de estos backdoors tener acceso libre al sistema dejándolo vulnerable para cualquier ataque fraudulento.

El principal objetivo de los backdoors es infectar a la mayor cantidad de computadoras posibles para luego poder utilizarlas en redes conocidas como redes zombies.

1.3.13 Redes de Bots (Botnet)

Se define a las Redes de bots "Botnet" al conjunto de equipos infectados con un tipo de malware que permite controlarlos para uso del creador en forma de red.

En una primera instancia, los creadores de la botnet distribuyen el malware para infectar a los usuarios. Cada sistema infectado abre puertas traseras en el sistema, necesario para dar control al dueño de la botnet. Una vez que los equipos ahora bautizados zombies han sido reclutados, los creadores hacen uso de un centro de Comando y Control para llevar a cabo las tareas que deseen, utilizando de los recursos de todos los equipos que forman parte de la red.

Cuando un sistema es parte de una botnet los atacantes están en la capacidad de utilizar los recursos de todos los sistemas en la red para llevar a cabo acciones maliciosas. Las mismas que son realizadas en forma transparente al usuario mientras utiliza el equipo, pudiendo percatarse de esto solamente en caso de un consumo excesivo de recursos, el cual ralentizaría el funcionamiento o, incluso, impide su utilización.

Entre los usos fraudulentos que se dan las botnet se encuentran:

- El alquiler de la botnet para realizar alguna acción ilegal.
- Utilizarlas para realizar ataques de DDoS (Denegación de Servicio Distribuido), distribución de spam, etc

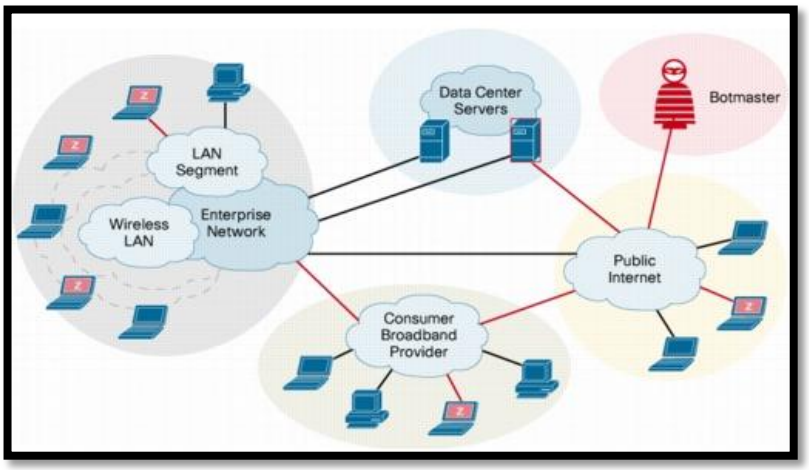


Figura 8: Botnet típica con computadores zombies en distintas localidades.
Fuente: http://www.cisco.com/en/ networking_solutions_whitepaper.html.

1.3.14 Keyloggers

Es un programa que registra y graba todas las pulsaciones de teclas y clics en la PC mientras se encuentra ejecutando, su funcionamiento es transparente al usuario debido a que se necesita pulsar combinaciones personalizadas de teclas para ingresar a su consola de configuración e incluso puede ocultarse de los menús donde se puede desinstalar o quitar los programas del sistema operativo.

Hay una gran cantidad de este tipo de programas que aparte de almacenar las pulsaciones tienen una gran variedad de módulos que de acuerdo al fabricante muestran la información de diversas formas como por ejemplo almacenar actividad por aplicación, hacer capturas de pantalla para capturar claves en los teclados digitales.

Algunos de estos programas también son capases de, una vez recolectada la información enviarla por e-mail a una cuenta de correo previamente ingresada por la persona que lo instalo el software.

Aunque lo expuesto habla de Keyloggers en software, cabe también mencionar la existencia de Keyloggers físicos que se colocan entre el teclado, el mouse y la computadora.

Figura 9: Keylogger Físico y mediante software. Curso de seguridad informática ESET.
Fuente: http://www.eset-la.com/centro-amenazas/educacion.php

1.3.15 Ransomware

El término en idioma inglés "ransom" se lo define como la exigencia de un pago por la libertad de alguien o de un objeto, lo que en castellano se traduciría como rescate. Si a este término se añade la palabra software obtenemos el nuevo término “Ransomware” del cual se obtendría la definición de secuestro de archivos a cambio de un rescate.

Reciben este nombre cualquier software con objetivos dañinos que mediante distintas técnicas imposibilitan al creador o dueño de un documento acceder al mismo. Este tipo de software tiene la capacidad cifrar con clave documentos y después deja instrucciones al usuario de cómo recuperarlos pero posterior al pago de un "rescate" monetario.

1.3.16 Spam

El Spam no es más que todo el correo electrónico no deseado que llega diariamente a nuestras cuentas de correo. Entre los principales objetivos está el de ofrecer por una parte productos y servicios que por lo general son de gran impacto a más de tener precios accesibles. Por otro lado también hacer llegar información muy variada como por ejemplo historias, noticias, humor, etc. Pero según estadísticas el 4% del correo no solicitado logra

su principal objetivo y los usuarios terminan adquiriendo los productos, contratando los servicios o entregando información confidencial.

El Spam ha tenido un gran éxito los últimos años, porque muchas empresas utilizan este mecanismo para publicitar sus productos a un bajo costo en relación al costo de contratar publicidad en forma tradicional el ahorro se calcula en inferior hasta 100 veces en algunos casos. Los spammers (personas dedicadas al envió de spam) obtienen sus ganancias al alquilar sus bases de datos y su red de distribución para enviar correos a todos los usuarios que tienen almacenados.

- Para recolectar los correos de usuarios reales y alimentar sus bases de datos los spammers realizar distintas actividades como:
- Enviar las bien conocidas cadenas (hoax) de correos electrónicos
- Recolectar direcciones publicadas en foros, páginas web, etc.
- Correos formados por la combinación de letras tomadas aleatoriamente (Ej: aaa@mail.com, aab@mail.com) así después de algunos intentos se lograra obtener direcciones válidas.

Entre los principales perjuicios que causa el spam es:

- Afectar al ancho de banda el cual afecta en mayor número a las empresas
- Reducir la productividad de los empleados.
- Es uno de los medios más eficientes para hacer fraudes
- Ocasiona perdida de información real, debido a que si llenan un buzón de correo se puede perder información de verdadero interés
- Aumentan los falsos positivos al momento utilizar filtros de seguridad

Es un costo monetario ya que se “paga” por recibir el spam (pago por el servicio de internet, en algunos casos el servicio de correo, se consume ancho de banda, se consume tiempo del empleado que utiliza para leerlos, etc.)

Figura 10: Correo electrónico que contiene un mensaje de Spam. Curso de seguridad informática ESET.
Fuente: http://www.eset-la.com/centro-amenazas/educacion.php

1.3.17 Hoax

Las conocidas cadenas (Hoax) no representan una amenaza a primera vista pero se los clasifica de forma separada porque suelen utilizarse para robar y recolectar direcciones de correos y no para realizar fraudes directamente.

Su contenido es variado y se han convertido en una verdadera epidemia ocupando mucho del espacio disponible en los buzones de nuestras cuentas de correo electrónico tomando ventaja de que los mismos usuarios se encargar de enviarlas a todos sus contactos siguiendo la recomendación de la cadena.

Entre sus características están:

- Todas llevan un texto al final como "envía este correo a X personas" o textos similares.
- En su texto central encontramos texto que va desde inofensivo, humor, noticias hasta engaños o alertas.

- La mayor cantidad de los mensajes incluyen alertas son sobre virus informáticos, promociones especiales, ayuda a personas, etc.
- Sus principales objetivo es recolectar el mayor número de direcciones de correo reales.
- Es común recibirlas con cientos de contactos
- Este tipo de mensajes explotan la llamada Ingeniería Social así mediante diversas metodologías convencen al usuario que debe enviar la cadena a un grupo de contactos. Puede apreciarse que es muy fácil recolectar direcciones de correo electrónico y como ya fue mencionado antes es una técnica muy utilizada por los spammers para recolectar la mayor cantidad de direcciones válidas.

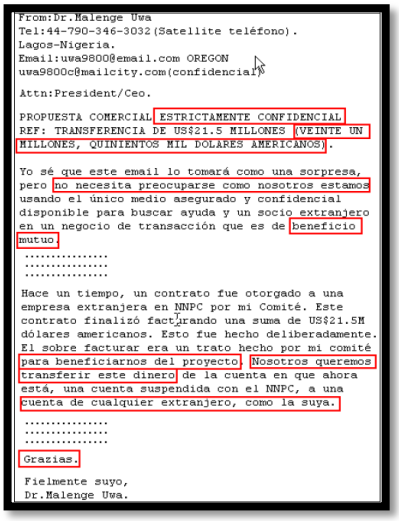
1.3.18 Scam

El Scam (estafa en inglés) se emplea para designar el intento de estafa a través del correo electrónico. El Scam es una mezcla de Spam y Hoax que persiguen un fin delictivo y generalmente contienen información relacionada a donaciones, loterías y comisiones.

Las versiones originales se Scam eran enviadas vía fax, pero con la facilidad del correo electrónico que a más de ser económico tiene un gran nivel de confidencialidad. Generalmente los fondos son canalizados fuera del país de origen donde son pedidas las donaciones.

El país donde comenzó esta técnica fue Nigeria donde se lo conoce como el 419 por el número de artículo del código penal en ese país.

También existen correos donde solicitan ciertos datos confidenciales como información de cuentas bancarias donde con promesas de que se traspasaran comisiones por concepto de negocios de oportunidad o inversiones de alta rentabilidad.



From:Dr.Malenge Uwa
Tel:44-790-346-3032(Satellite teléfono).
Lagos-Nigeria.
Email:uwa9800@email.com OREGON
uwa9800c@mailcity.com(confidencial)

Attn:President/Ceo.

PROPUESTA COMERCIAL ESTRICTAMENTE CONFIDENCIAL
REF: TRANSFERENCIA DE US$21.5 MILLONES (VEINTE UN MILLONES, QUINIENTOS MIL DOLARES AMERICANOS).

Yo sé que este email lo tomará como una sorpresa, pero no necesita preocuparse como nosotros estamos usando el único medio asegurado y confidencial disponible para buscar ayuda y un socio extranjero en un negocio de transacción que es de beneficio mutuo.

Hace un tiempo, un contrato fue otorgado a una empresa extranjera en NNPC por mi Comité. Este contrato finalizó facturando una suma de US$21.5M dólares americanos. Esto fue hecho deliberadamente. El sobre facturar era un trato hecho por mi comité para beneficiarnos del proyecto. Nosotros queremos transferir este dinero de la cuenta en que ahora está, una cuenta suspendida con el NNPC, a una cuenta de cualquier extranjero, como la suya.

Gracias.

Fielmente suyo,
Dr.Malenge Uwa.

Figura 11: Mensaje Scam estafa Nigeriana. Curso de seguridad informática ESET.
Fuente: http://es.wikipedia.org/wiki/Estafa_nigeriana

1.3.19 Phishing

El Phishing es un mensaje de correo electrónico que simula ser enviado principalmente por una entidad financiera con el fin de engañar a los destinatarios haciéndoles creer que el de una fuente legitima y que proviene de dicha entidad de confianza.

El cuerpo del mensaje informa que se han perdido o se van a actualizar datos personales del usuario e invita a los destinatarios a ingresar al enlace que se añade en el mensaje donde se pide completar formularios con información confidencial.

Si el usuario es engañado por el mensaje, ingresara al enlace de la página web falsa la cual es idéntica a la original de la institución correspondiente y allí el usuario confiado de la veracidad del sitio entregara todos sus datos personales a los creadores del correo Spam y el sitio. Normalmente se envía un correo Spam que es utilizado con fines delictivos para

obtener de forma fraudulenta información confidencial del usuario por medio de estas páginas señuelo.

El problema del Phishing es el daño monetario que puede causar por que el usuario al entregar información confidencial de su cuenta bancaria, los cibercriminales tienen el acceso completo al sitio real de la institución financiera donde con gran facilidad pueden transferir los fondos a cuentas de su propiedad y en el caso de las tarjetas de crédito realizar cualquier consumo o compras que deseen.

En el caso de haber entregado información confidencial pueden usar la misma para realizar fraudes o estafar a la víctima.

La industria del Phishing es tal que incluso se venden "kits" donde se indica a detalle cómo realizar estos ilícitos y estafas de este estilo.

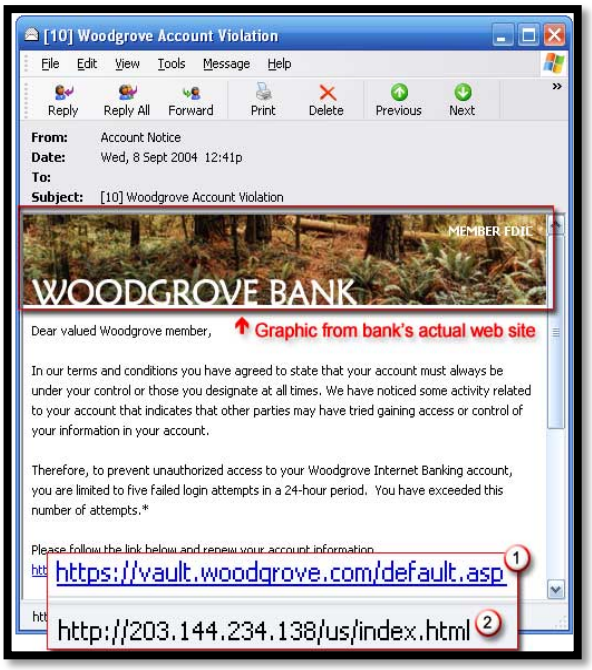


Figura 12: Mensaje Phishing, donde se puede apreciar le vinculo al sitio fraudulento de un banco.
Fuente: http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx

1.3.20 Spyware

El Spyware (Spy Software) es un software espía que recopila información sobre las actividades de PC's de personas u organizaciones sea consentida o no. Este malware utilizado principalmente por empresas publicitarias de internet.

Actualmente es uno de los tipos de malware de mayor difusión con elevada presencia en ambientes empresariales y de hogar. Esto es principalmente debido a que se instalan con otras aplicaciones que son de utilidad al usuario unas con consentimiento al momento de la instalación pero la gran mayoría no. Estadísticas demuestran que hoy en día existen más versiones de spyware que versiones de virus.

Inicialmente el spyware nació como un conjunto de aplicaciones incluidas junto al software gratuito con el objetivo de conocer los intereses de navegación por internet. Toda esta información recopilada es de gran valor para empresas dedicadas al marketing por internet ya que gracias a estos informes pueden determinar los perfiles de los usuario almacenados en sus bases de datos y así generar aplicaciones de interés o enviar e-mails con información de acuerdo al perfil de cada usuario.

Los spyware incrementaron sus funcionalidades hasta convertirse en algo más que programas ocultos que procuran obtener información, hoy en día intentan interactuar con el usuario a través de barras de herramientas en el navegador o simulando tener alguna funcionalidad.

Pero uno de los grandes problemas que genera el spyware, además de la clara invasión a la privacidad, es el mal consumo de recursos en red, debido a la constante comunicación que mantienen con sitios no deseados.

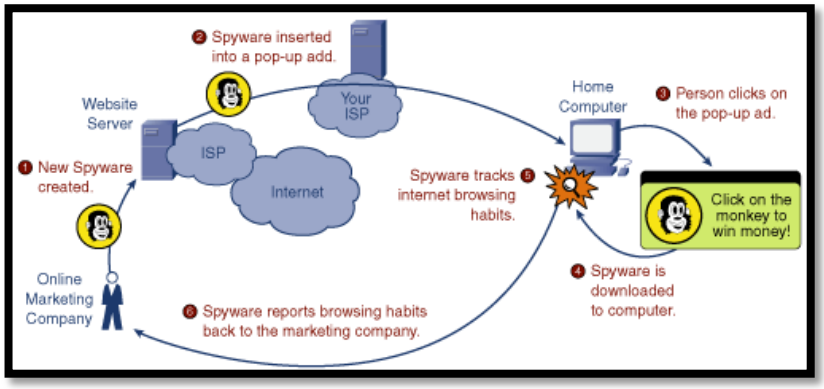


Figura 13: Ejemplo de un programas Spyware que es instalado mediante un popup.
Para hacer investigación de mercado de empresas de Marketing.
Fuente: http://www.sbunit.com/spyware.html

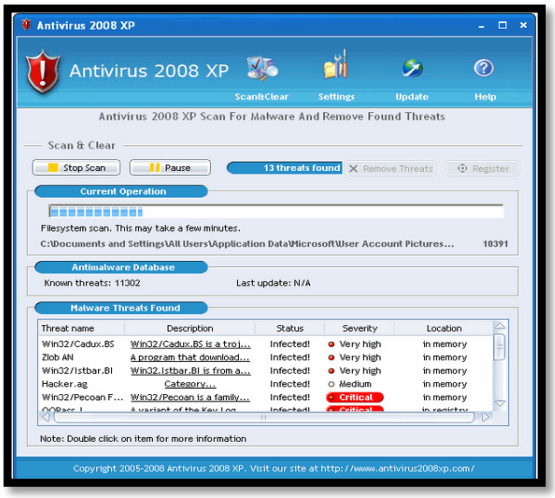


Figura 14: Ejemplo popup Spyware.
Ofreciendo servicio gratuito de limpieza de virus detectados en el computador.
Fuente: http://www.computerrepairsny.com/base.htm

1.3.21 Adware

El Adware (Advertised Software) es un software que despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla.

Algunos programas Adware son también shareware en estos los usuarios tiene la opción de pagar por una versión registrada o con licencia, que normalmente elimina los anuncios.

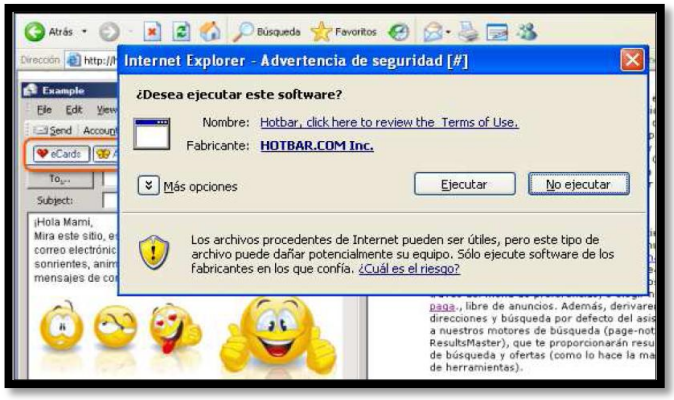


Figura 15: Instalación de Hotbar. Curso de seguridad informática ESET.
Fuente: http://www.eset-la.com/centro-amenazas/educacion.php

Figura 16: Hotbar instalada. Curso de seguridad informática ESET.
Fuente: http://www.eset-la.com/centro-amenazas/educacion.php

1.3.22 Ingeniería Social

El factor humano es considerado como el eslabón más débil en la cadena de seguridad informática. Así la ingeniería social ataca a esta vulnerabilidad para irrumpir en los sistemas de computadora ya que se basa en las relaciones interpersonales y el engaño. Debido a esto incluso las organizaciones con las más fuertes contramedidas de seguridad técnica, como procesos de autentificación, firewalls, etc. Pueden fallar en proteger sus sistemas.

Esto puede ocurrir si un empleado sin saberlo entrega información confidencial (Ej. contraseñas y direcciones IP) a terceras personas mediante llamadas telefónicas, e-mails con links a formularios o dejando esta información en lugares accesibles como pegada en la pantalla del PC.

El mejor medio de defensa para ataques de ingeniería social es un programa continuo de concientización e importancia de la seguridad informática en la organización, donde todos los empleados y terceras personas que tengan acceso a las facilidades de la organización, serán educados sobre los riesgos involucrados en caer en este tipo de ataques.

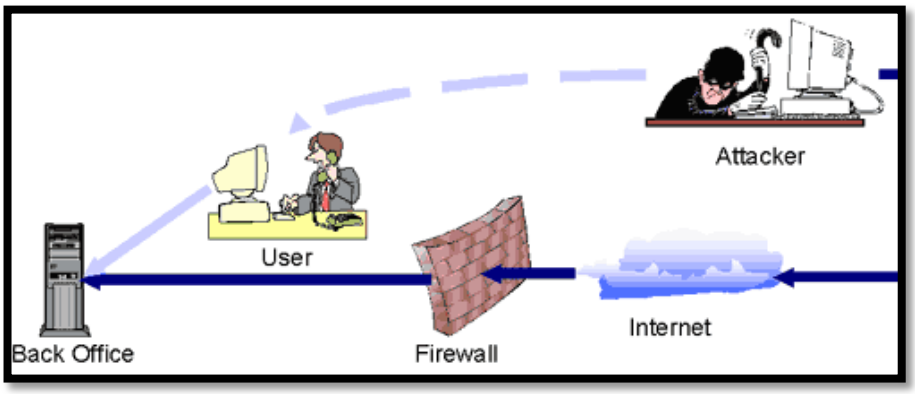


Figura 17: La ingeniería social se basa en la manipulación de los usuarios y no irrumpiendo la tecnología de seguridad utilizada por sus organizaciones.
Fuente: http://articles.techrepublic.com.com/5100-10878_11-1047991.html

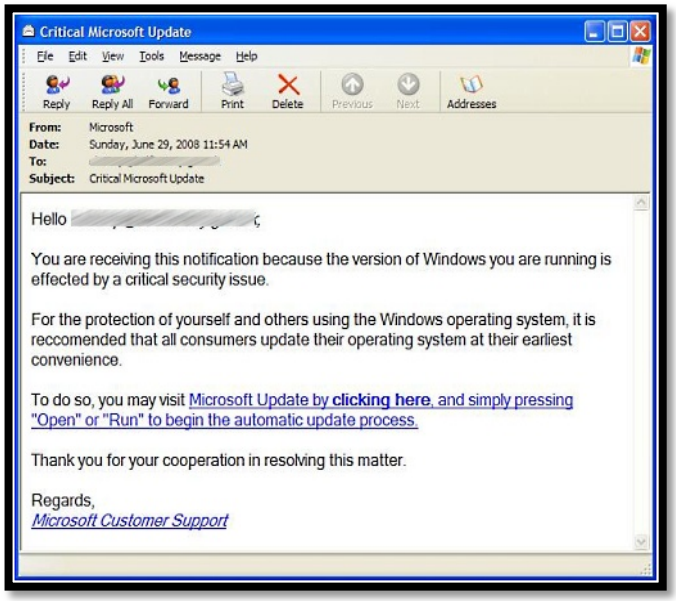


Figura 18: Mensaje de correo electrónico que utiliza técnicas de ingeniería social.
Fuente: http://securitylabs.websense.com/content/Alerts/3122.aspx

1.4 Problemas del Crimen Informático

Los sistemas informáticos pueden ser usados para robar dinero, mercancías, software o información corporativa. También pueden cometerse crímenes cuando los datos de aplicaciones de negocio son manipulados para realizar transacciones falsas o no autorizadas. La simple visualización de los datos puede proveer al criminal suficiente información para robar ideas confidenciales. Un criminal informático toma ventaja de que su crimen se efectúa sin que nada sea físicamente tomado o robado.

Debido a que gran parte de los sistemas informáticos están conectados a las redes WAN o a la internet para criminales especializados es muy fácil ingresar mediante acceso remoto, así la escena del crimen podría estar en cualquier parte del mundo lo cual hace más difícil la investigación y llegar a conocer a los responsables de un crimen cibernético.

Entre las principales amenazas de los crímenes informáticos están[5]:

- **Pérdida financiera:** Pueden ser directas, mediante fondos electrónicos o indirecta, mediante perdida de información confidencial o falta de continuidad del negocio.
- **Pérdida de credibilidad o ventaja competitiva:** Muchas organizaciones en especial bancos, cooperativas de ahorro, fondos de inversión, necesitan tener una gran credibilidad y mantener la confianza de sus clientes así como al público en general para mantener su ventaja competitiva. Una violación de la seguridad como ataques a su base de datos, su página web, etc. Puede afectar seriamente la

[5] **Texto tomado de:** LAWTON, Lynn; JONSON, Robert. *Manual de Preparación al Examen CISA 200* [en línea]. ISACA, 2007, 42008, [citado 10-12-2009], Formato pdf, Disponible en Internet: http://www.isaca.org/cisajobpractice.

credibilidad de la organización en consecuencia puede llevar a pérdida de clientes y su prestigio que muchos años les costó conformar.

- **Chantaje y espionaje industrial:** Un criminal puede extorsionar con pagos económicos a una organización amenazando con entregar públicamente información confidencial de la organización, la cual obtuvo aprovechando las brechas de seguridad que tenía la organización para ingresar a su red y tomarla.

  El criminal también puede obtener réditos económicos al entregar a empresas competidoras o venderlas al mejor postor la información obtenida fraudulentamente.
- **Revelación de información confidencial**: Como ya fue señalado este tipo de información puede afectar gravemente a una organización y su negocio. Debido a que pueden ser afectadas incluso por acciones legales y regulatorias en el caso de la organización haya cometido algún acto ilegal.
- **Sabotaje:** No todos los criminales buscan obtener ganancias financieras. Algunos solamente quieren causar daño porque les desagrada la organización, motivos filosóficos, políticos o solo por el hecho de gratificarse al aplicar sus conocimientos y causar daño a la organización.

Entre las personas que con frecuencia se aprovechan de vulnerabilidades de seguridad se encuentran tanto personal interno como externo a la organización entre los que se puede clasificar:

- **Hackers:** Personas con habilidades técnicas muy avanzadas tanto de lenguajes de programación como de manejo de sistemas operativos cliente y servidor. Este tipo de personas típicamente trata de probar los límites de las restricciones de acceso a los sistemas como prueba de sus habilidades al sobrepasar las seguridades. Algunos no tienen intención de causar daño a los sistemas pero en el proceso de violentar las seguridades causan daños.

Existen también activistas que causan daños impulsados por creencias políticas o filosóficas las cuales según ellos justifican sus acciones así infrinjan la ley. Y finalmente existen hackers que tienen como objetivo cometer fraudes para cometer obtener réditos monetarios.

En la actualidad los términos hacker y cracker se usan indistintamente pero se tiene que tomar en cuenta sus diferencias como que un hacker accede a los sistemas por diversión o por probar sus conocimientos mientras que un cracker es una persona que quiere causar daño y obtener rédito de la intrusión a un sistema.

- **Script kiddies:** Se refiere a personas que usan programas escritos por otros para realizar sus actividades fraudulentas de intrusión a los sistemas; a menudo son incapaces de escribir programas similares por cuenta propia.
- **Crackers:** Personas que tratan de violentar las seguridades de los sistemas para tener acceso no autorizado con objetivos fraudulentos.
- **Empleados (autorizados y no autorizados):** Son miembros de la organización a quien se les entrego acceso al sistema en relación de su puesto de trabajo. Se debe tener presente que el personal de la organización puede causar daño considerable a los sistemas sino se les entrega accesos controlados y también filtrar a ex empleados para que dejen de tener acceso al sistema una vez abandonada la organización.

  Es importante concientizar a los empleados activos la importancia de mantener sus claves en lugares seguros y no entregarlas a terceras personas. Ya que mediante estas claves se pueden cometer fraudes o crímenes informáticos dejando como culpable al dueño del acceso y no a los verdaderos culpables.
- **Personal de Sistemas:** Debido a la característica de su trabajo este personal tiene acceso a todo el sistema y a la información que se contiene en el mismo. El uso de

controles lógicos es importante para mantener una bitácora de acceso al sistema así se evitara violaciones y robo de información por parte de este personal.

- **Usuarios finales:** Son todos los usuarios del sistema quienes manejan los programas de ofimática y el software a medida desarrollado para la organización.
- **Ex empleados:** Es de vital importancia eliminar el acceso al sistema de estas personas en especial sino se termina en los mejores términos debido a que los mismos podrían tomar represalias y afectar información delicada de la organización
- **Personas ajenas a la organización:** Competidores, terroristas, criminales, hackers.
- **Personal a tiempo parcial o temporal:** Es importante tener en cuenta a quien se brinda acceso a las oficinas por que el personal de limpieza o de mantenimiento tiene acceso total a todas las oficinas y en horarios donde el personal no está presente así al no tener un adecuado control de seguridad en los sistemas se corre un gran riesgo con la información de la organización.

Crímenes de Computadora		
Fuente del Ataque	**Objetivo del Ataque**	**Ejemplos**
La computadora es el objeto del crimen: **El cyber criminal usa computadoras de terceras personas para lanzar un ataque**	Computadora especifica utilizada como medio de ataques a terceros	- Denegación de servicio - Hacking
La computadora es el sujeto del crimen: **El cyber criminal usa su computadora para cometer un crimen con el objetivo es atacar otras computadoras**	El objetivo puede o no ser definido. El cyber criminal lanza el ataque sin un objetivo específico en mente	- DoS Distribuido - Virus
La computadora es la herramienta del crimen: **El cyber criminal usa la computadora para cometer el crímenes pero el objeto no es la computadora**	El objetivo son los datos o la información en la computadora	- Fraudes - Acceso no autorizado - Phishing
La computadora simboliza el crimen. **El cyber criminal engaña al usuario de computadoras para obtener información confidencial**	El objetivo es obtener información confidencial del usuario	Métodos de ingeniería social como: - Sitios web falsos - Phishing - Correos fraudulentos - Correos chatarra - Falsos resúmenes para empleo

Tabla 3: Tabla de resumen crímenes de computadoras.
Fuente: Hugo Paredes. **Fecha de elaboración:** Febrero 2010.

1.5 Buenas Prácticas de Seguridad Informática

Es necesario que tanto administradores como usuarios de un sistema incorporen buenas prácticas de seguridad informática para proteger su entorno de trabajo o estudios, para evitar formar parte del grupo global de potenciales y eventuales víctimas de cualquier amenaza circulante que no solo buscan vulnerabilidades en los sistemas sino también sacar provecho de la ignorancia de usuarios e incluso administradores de red al desconocer o no

poner en práctica nociones básicas de seguridad informática. Pero para crear una verdadera conciencia se deben conocer los peligros a los que se puede estar expuesto y como detenerlos a tiempo mediante los distintos mecanismos de prevención como:

- Impacto de las amenazas
- Instalación y configuración del sistema operativo
- Mantener actualizado el sistema operativo y las aplicaciones
- Seguridad cliente servidor
- Seguridad de la red
- Controles de seguridad para internet
- Manejo y Protección de claves

1.5.1 Impacto de las amenazas[6]

Es difícil determinar con exactitud como las amenazas informáticas ya descritas anteriormente pueden afectar a una organización, pero se puede determinar generalidades como las siguientes:

- Pérdida de ingresos monetarios al detenerse el sistema de la organización
- Mayor costo en mantenimiento y recuperación (Corrigiendo información y restableciendo servicios)
- Perdida de información (Datos críticos, información propietaria, contratos)
- Perdida de secretos comerciales

---

[6] CISA Texto tomado de: LAWTON, Lynn; JONSON, Robert. *Manual de Preparación al Examen CISA 200* [en línea]. ISACA, 2007, 42008, [citado 10-12-2009], Formato pdf, Disponible en Internet: http://www.isaca.org/cisajobpractice.

- Daño a la imagen de la organización
- Desempeño reducido de los sistemas y servicios de la red
- Incumplimiento con leyes y regulaciones (En el caso de ser organizaciones que pasan por auditorias informáticas)
- Incumplimientos de compromisos contractuales
- Acción legal de parte de clientes por pérdida de datos confidenciales e incumplimiento de contratos o servicios.

1.5.2 Instalación y configuración

Es común mencionar que para instalar un sistema operativo solo hace falta el medio físico o de red para instalarlo y después realizar la configuración "Siguiente" ,"Siguiente". Si bien esta configuración en muchos de los casos es la preferida debemos recordar que nuestro trabajo no termina en eso momento por el contrario solo es el comienzo de varios pasos de configuración para que el sistema sea seguro. Entre las pautas para dar un mejor "blindaje" por así decirlo a la configuración por defecto de nuestro sistema se podrían enumerar en (Como base un sistema operativo Windows XP con Service Pack 2 o Service Pack 3, totalmente limpio sin actualización de ningún tipo):

- Verificar que el firewall se encuentre habilitado. Esto en principió es importante ya que existen 65.536 puertos en una PC, de los cuales se utilizan una pequeña cantidad, mantenerlos abiertos todos es incensario mantenerlos abiertos es una invitación a ser atacados por intrusos (Personas o Software Malicioso). Existen excepciones que pueden ser configuradas en caso de necesitar dar acceso a programas específicos y es mejor configurarlas que solo deshabilitar el firewall.
- Así el computador este en una red segura siempre se debe tener habilitada una protección antivirus actualizada ya que los ataques pueden venir de forma inesperada.

- Debido a que en sistemas como Windows XP, el usuario Administrador está habilitado por defecto cualquier usuario tendría permiso de realizar cualquier modificación y sería mucho más fácil para el malware causar daño en este tipo de cuentas del sistema operativo. Por lo cual es importante manejar un controlador de domino para que los usuarios tengan permisos restringidos y en el caso de no tener un controlador de dominio es necesario configurar políticas de restricción locales o crear cuentas limitadas.
- Al tener computadores en red es común utilizar recursos compartidos debido a esto es recomendable colocar contraseñas para evitar la reproducción de ciertos tipos de malware que se aprovechan de las carpetas compartidas.
- Se debe controlar periódicamente los registros de Windows, los programas instalados y los programas de inicio, para evitar que cualquier tipo de malware se esté ejecutando causando luego fallas al sistema, elimine o contamine los documentos en el computador.
- Los puntos de restauración del sistema son importantes para poder rescatar al sistema en el caso de fallas graves en el sistema.

1.5.3 Mantener actualizado el sistema operativo y las aplicaciones

Debido a que el malware en su gran mayoría es diseñado para atacar vulnerabilidades es importante mantener las actuaciones lo más al día posible, tanto en los sistemas operativos como en las aplicaciones.

Códigos maliciosos como Slammer, Sasser o Conficker, detectados en los años 2003, 2004 y 2008 respectivamente, infectaban los sistemas a través de vulnerabilidades que no habían sido debidamente corregidas mediante sus respectivas actualizaciones.

Así para mantener un sistema debidamente actualizado se deben tener medidas prácticas de prevención como:

- No descargar actualizaciones de sitios que no sean del respectivo fabricante es decir hacerlo solo de sitios de confianza. Actualizaciones de otros sitios podrían no ser precisamente la actualización deseada y contener código malicioso extra adjuntado a la actualización.
- Descargar las actualizaciones mediante mecanismos ofrecidos por los fabricantes. Como en el caso de productos Microsoft, que provee mecanismos de actualización en segundo mediante herramientas incluidas por defecto en los sistemas operativos.

En plataformas Microsoft se permite:

- Acceder a sitios web de confianza como Windows Update para obtener los últimos parches de seguridad
- Configuraciones mediante aplicaciones dedicadas de seguridad como en el caso de Windows XP el Centro de Seguridad de Windows, donde se puede configurar cuando y como realizar las actualizaciones.
- Utilizar herramientas gratuitas como WSUS (Windows Server Update Services) donde se puede centralizar las actualizaciones.

En todo entorno corporativo es de vital importancia sin importar la plataforma utilizada, preparar políticas de gestión de actualizaciones claras, que permitan coordinar y administrar las actualizaciones de seguridad tanto para sistemas operativos y aplicaciones de forma centralizada y ordenada.

Para evitar molestias en los usuarios y falta de continuidad del negocio.

Figura 19: Centro de seguridad de Windows. Curso de seguridad informática ESET.
Fuente: http://www.eset-la.com/centro-amenazas/educacion.php

1.5.4 Seguridad Cliente-Servidor

Un sistema Cliente-Servidor contiene numerosos puntos de acceso. Aun así los procedimientos de seguridad para entornos donde se utilizan servidores no son por lo general bien definidos ni están debidamente protegidos. Los sistemas Cliente-Servidor utilizan técnicas distribuidas generando un mayor riesgo de ataques a los datos y a las aplicaciones utilizadas en la organización. Para asegurar con eficacia la seguridad en ambientes Cliente-Servidor, se deben identificar todos los puntos de acceso, permisos e identificar que aplicaciones tienen procesamiento centralizado porque estas utilizan una ruta predefinida para tener acceso a los recursos necesarios para efectuar su trabajo.

Debido a que existen varias rutas de acceso al Servidor cada una de estas debe ser examinada de manera individual e investigar si existen relaciones entre ellas. Es importante asegurar que no hayan quedado accesos sin identificar ya que los mismos podrían ser utilizados posteriormente para ataques y serian difícil de encontrar por que no fueron

identificados a tiempo. Para aumentar la seguridad en un entorno Cliente-Servidor, se debe manejar técnicas de control como las siguientes:

- Asegurar la seguridad de los datos o aplicaciones de entornos Cliente-Servidor, se puede lograr esto deshabilitado las unidades de floppy, CD o DVD y las unidades extraíbles USB. Las estaciones de trabajo sin estos accesos impiden que el software de control instalado sea evadido por medio del uso de aplicaciones de terceros traídas del exterior de la organización lo que en el caso de ocurrir haría que la estación de trabajo sea vulnerable a accesos no autorizados. Asegurando los archivos de arranque (Boot) o de carga (Start up), impedirían que usuarios no autorizados eludan comandos de registro de entrada y logren acceso.
- Los dispositivos de monitoreo de red pueden ser usados para inspeccionar la actividad proveniente de usuarios conocidos o desconocidos. Estos dispositivos pueden identificar direcciones IP de los clientes, permitiendo la terminación de sesiones en forma proactiva así como también encontrando evidencia de acceso no autorizado para posteriores investigaciones. Sin embargo los métodos de aseguramiento del ambiente Cliente-Servidor solo pueden ser eficaces en la medida que existan las herramientas y que el administrador lleve un adecuado monitoreo de los mismos. Como un control de detección de accesos, si el administrador de la red no monitorea o no mantiene una adecuada lectura de los mismos, la herramienta se vuelve inútil contra intrusos no autorizados y así sean detectados no existe la persona que deshabilite o investigue el acceso.
- Técnicas de encriptación de datos o de permisos de acceso a carpetas de respaldos pueden ayudar a proteger los datos sensibles de la organización contra accesos no autorizados.

- Los sistemas de autentificación pueden proveer a todo el entorno Cliente-Servidor, facilidades lógicas que puedan diferenciar a los usuarios de la organización. Otro método es la utilización de tarjetas inteligentes (Smart Cards), que usan dispositivos manuales de hardware y técnicas de inscripción para identificar que solo los usuarios del sistema ingresen utilicen ciertas estaciones de trabajo o computadores portátiles.
- El uso de programas de control a nivel de aplicaciones se pueden utilizar para restringir, limitar acceso a información o la utilización ciertas funciones dejando solo lo necesario según el perfil del usuario. El control de acceso consigue que la estación de trabajo sea enfocada en tareas productivas y permiten administrar la seguridad Cliente-Servidor de forma más sencilla.

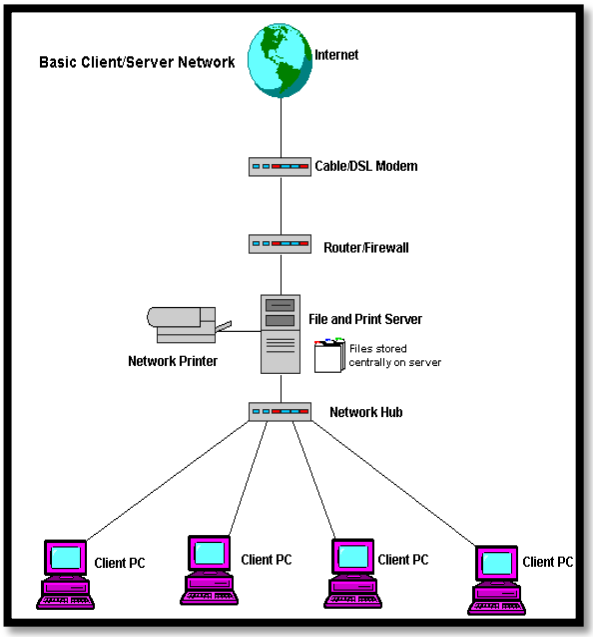


Figura 20: Configuración básica de una red cliente servidor.
Fuente: http://www.computertipsntricks.com/nt_CSnetwork.htm

1.5.5 Seguridad de la red

Una red segura es base fundamental para que cualquier organización tenga un entorno Cliente-Servidor confiable. Existe gran cantidad de amenazas a la red que se deben tener presentes, todos los ataques se basan primero en un escaneo del funcionamiento y de la información que pasa por la red. Los ataques pueden ser pasivos a activos, pero los ataques pasivos son el primer paso de un ataque activo para realizar intrusiones en la red de la organización.

Ataques Pasivos

Los ataques pasivos reúnen información de la red con técnicas como las descritas a continuación:

- **Análisis de Red:** El intruso aplica un método sistemático y metódico conocido como "footprinting" para crear un perfil completo de la infraestructura de seguridad de la red de la organización que está atacando. Durante esta fase inicial de reconocimiento, el intruso usa una combinación de herramientas y técnicas para crear un depósito de información sobre la red interna. Esto incluirá probablemente información sobre alias de inicio de sesión, funciones de red, direcciones IP internas, Gateways y Firewalls. Después determina cuál es su sistema objetivo por lo general los servidores, el intruso explora los puertos del sistema para determinar qué servicios y que sistema operativo esta en operación para mediante esta información determinar las posibles vulnerabilidades y usarlas para realizar su ataque.
- **Eavesdropping (Termino Ingles: Escuchar secretamente):** EL intruso recoge información que fluye a través de la red con la intención de adquirir y liberar el contenido del mensaje para cualquier análisis personal o para terceros quienes podrían haber encargado dicha intromisión. Estos es particularmente significativo

cuando se considera que toda la información sensitiva que atraviesa por la red puede ser vista, incluyendo correo electrónico, contraseñas y en algunos casos, el uso de teclado en tiempo real. Estas actividades pueden permitir al intruso tener acceso no autorizado para usar esta información de manera fraudulenta. Por ejemplo cuentas de tarjetas de crédito y comprometer la confidencialidad de la información sensitiva que podría poner en peligro los activos financieros de una persona u organización e incluso afectar la reputación de una organización.

- **Análisis de trafico:** El intruso determina la naturaleza del flujo de tráfico entre los hosts definidos y por medio de un análisis de: longitud de la sección, frecuencia y la longitud del mensaje puede adivinar el tipo de comunicación que tiene lugar en la red y así determinar la información a interceptar, como por ejemplo mensajes encriptados.

Ataques activos

Una vez que se ha recogido la suficiente información de la red, el intruso lanzara un ataque real contra un sistema donde su objetivo es tomar el control total del sistema o parte de el para hacer que cierto código malicioso se ejecute. Este control se podría utilizar para entre otras cosas obtener acceso no autorizado y la posibilidad de modificar información o programas, ocasionando negación de servicios, escalando privilegios, y obteniendo información sensitiva para utilizarla en fines fraudulentos. Intrusiones como estas se conocen como ataques activos, debido a que estos afectan los atributos de integridad, disponibilidad y autentificación de la seguridad de la red. Las formas habituales de ataques activos son :

- **Ataques de fuerza bruta:** Un intruso lanza un ataque usando herramientas de cracking de contraseñas que son muy fáciles de conseguir en la web a bajo o

ningún costo para descifrar contraseñas encriptadas ganando acceso no autorizado a la red de la organización atacada.

- **Enmascaramiento:** El intruso toma la identidad de un usuario original del sistema. Utilizando este ataque el intruso puede ganar acceso a datos sensitivos o a recursos de la red que no están disponibles bajo identidades ajenas a la organización. La suplantación de identidad se realiza mediante la falsificación de la IP método conocido como Spoofing de IP. Al utilizar estos ataques se puede romper la seguridad del Firewall.
- **Phishing:** Este ataque afecta tanto al correo electrónico como sitios web reconocidos por los usuarios como seguros los mismos tratan de convencer al usuario que el sitio o los enlaces del correo electrónico son auténticos. Ataques como estos se realizan con la intención de obtener información para usos fraudulentos o de ingeniería social.
- **Modificación de mensajes:** La modificación involucra captura de un mensaje verdadero de la empresa u organizaciones de confianza para luego hacerle cambios, evitando que llegue a destino, cambiando su contenido o demorando su transmisión. Esto podría tener efectos desastrosos si por ejemplo el mensaje proviniera de una institución financiera solicitando pagos a sus clientes.
- **Acceso autorizado a través de internet o servicios basados en la web:** Muchos paquetes de software de internet contienen vulnerabilidades que vuelven a los sistemas susceptibles de ataques. Adicionalmente, muchos de estos sistemas son grandes y difíciles de configurar, dando como resultado un gran porcentaje de incidentes de acceso no autorizado. Entre los que se pueden incluir:
    - Alterar los enlaces entre las direcciones de IP y los nombres de dominio para personificar cualquier tipo de servidor.

- Liberar scripts que se pueden ejecutar con privilegios de administrador los cuales pueden por completo control de un servidor.
- La ejecución de scripts del lado del cliente (Applets Java o ActionScripts) presentan el peligro de ejecutar código malicioso directamente en el sistema operativo sin ninguna restricción.

- **Negación de servicio:** Los ataques de negación de servicio ocurren cuando una computadora conectada a internet es inundada con datos y/o solicitudes que deben ser atendidas. La máquina se dedica exclusivamente a atender estos mensajes y queda imposibilitada de realizar otras actividades. Al final de un ataque exitoso el recurso de red que fue atacado se paraliza y no queda disponible para los usuarios genuinos. Esta interrupciones comunes están:
  - Paralizar el contacto con Cliente-Servidor
  - Inundar la maquina con solicitudes falsas
  - Llenar al disco duro o la memoria con información duplicada e inservible
  - Aislar o negar es servicio DNS a los Clientes de la red.

1.5.6 Controles de seguridad para internet

Para establecer controles efectivos de seguridad para internet, una organización debe desarrollar controles dentro de un marco de seguridad a partir del cual se puedan implementar y soportar debidamente en relación de lo que dispone la organización. Generalmente, el proceso para establecer dicho marco es mediante políticas corporativas y reglas que tiene la organización para controlar el uso de internet.

Por ejemplo: Un conjunto de reglas debe tratar sobre el uso apropiado de los recursos de Internet con normas que puedan reservar privilegios de Internet a quienes tengan necesidades del negocio, definir qué recursos de información estarán disponibles para los

usuarios externos y definir en qué redes confiar y en cuáles no, dentro y fuera de la organización.

Otro conjunto de reglas que se debe tratar son la clasificación de la sensibilidad o criticidad de los recursos de información. Esto ayudara a determinar qué información estará disponible para uso en internet y los niveles de seguridad a considerar para los recursos corporativos. A partir de una evaluación de estos aspectos, una organización podrá desarrollar reglas específicas de seguridad para cada caso.

Por ejemplo: Se puede desarrollar reglas que hagan más estricta la seguridad del sistema operativo que definan como se debe configurar el sistema operativo detallen que servicios de internet deben ser bloqueados para usuarios externos en los que no se confía y definir como el sistema estará protegido por firewalls. Adicionalmente, se pueden definir procesos de control complementarios como:

- Concientización y entrenamiento sobre seguridad para los empleados, hecha a la medida de sus niveles de responsabilidad.
- Estándares de firewall y de seguridad para desarrollar e implementar arquitectura de firewall.
- Estándares de detección de intrusos y seguridad para desarrollar e implementar arquitecturas de IDS.
- Gestión de incidentes y respuesta para detección, contención y recuperación.
- Entorno o ambiente común de computadores de escritorio para controlar de forma automatizada la información que es presentada en los computadores de escritorio de los empleados.

- Monitoreo de las actividades o usos no autorizados de internet y notificación a los usuarios finales sobre los incidentes de seguridad por medio de boletines o alertas de forma entendible para usuarios finales.

1.5.7 Manejo y creación de claves

Actualmente, el uso de claves es común para cualquier usuario de un computador y es como nos autentificamos en la organización. Es decir que se usan contraseñas para asegurar que una persona es dueña de un equipo o que pertenece a una organización. Si otra persona dispone de dichas credenciales puede afirmar ser quien no es, lo que comúnmente conocemos como suplantación de identidad. No siempre tomamos la importancia de una clave y tratamos de que sea la más fácil de usar pero se puede seguir ciertas normas para lograr esto sin que la clave sea fácil de descifrar.

Pero, ¿Por qué es importante utilizar una clave segura y no es lo mismo cualquier palabra que nos facilite la vida porque nunca la olvidamos?

La respuesta son los denominados diccionarios, ya que así como cada idioma posee su diccionario, cada atacante puede conseguir uno fácilmente en internet o tener uno propio. Esto es un archivo de palabras que son de uso común en cualquier idioma, con miles de combinaciones posibles de las mismas. Es decir, que en estos archivos existe cualquier palabra que nos podamos imaginar. Por eso, es tan importante seguir consejos para crear una contraseña segura como:

1.- No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, ciudades, u otro relacionado).

2.- No usar contraseñas completamente numéricas con algún significado (números telefónicos, fecha de nacimiento, placa del automóvil, etc).

3.- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.

4.- Deberían tener entre 6 y 8 caracteres de longitud (como mínimo).

5.- Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.

6.- Deben ser fáciles de recordar, para no verse obligado a escribirlas y difíciles de descifrar.

Aunque algunas de estas recomendaciones pueden ser fácilmente configuradas mediante políticas de grupo en entornos que manejan directorio activo, muchas de estas recomendaciones suelen ser configuradas para evitar utilizarlas debido a que sus usuarios olvidan fácilmente las claves o simplemente no tienen cuidado con las mismas pero un administrador no puede configurar un entorno seguro si normas de seguridad básicas no son tomadas en cuenta por mandos más altos en la organización quienes suelen pedir realizar dichas configuraciones a los administradores.

Protección de la clave

La protección de la contraseña recae tanto sobre el administrador del sistema como sobre el usuario. Al comprometer las credenciales de una cuenta se puede estar comprometiendo todo el sistema.

Así se podría decir que: “Una clave debe ser como un cepillo de dientes. Se usa cada día; se debe cambiar regularmente; y no se comparte con tus amigos”.

Algunas consideraciones a seguir principalmente por los administradores son:

1.- No permitir ninguna cuenta sin contraseña.

2.- No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas de Root, System, Test, Demo, Guest, en blanco, etc.

3.- Nunca compartir con nadie la contraseña. Si se hace, cambiarla en lo posible inmediatamente.

4.- No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.

5.- No teclear la contraseña si hay alguien mirando. Es de buena educación de un usuario no mirar el teclado mientras alguien teclea su contraseña.

6.- No enviar la contraseña por correo electrónico, ni mencionarla en una conversación. Si es el caso no se debe mencionar, explícitamente diciendo: “mi clave es...”.

7.- No mantener una contraseña indefinidamente. Cambiarla regularmente. Disponer de una lista de contraseñas que puedan usarse cíclicamente.

8.- Evitar la utilización de la misma contraseña sobre múltiples sistemas ya que si la misma es rota, entonces todos los sistemas que la utilicen se verán comprometidos.

Por supuesto un administrador no debe convertirse en un policía que lo controla todo con mano de hierro por así decirlo. El administrador debe ensañar la importancia de utilizar contraseñas seguras a los usuarios y no crear una conciencia paranoica, sino más bien indicarle que eso dará seguridad a su estación de trabajo evitando tener contratiempos que causen problemas cuando más necesite de su herramienta de trabajo que es ahora el computador en las organizaciones.

1.5.8 Honeypots y honeynets.

Honeypot es una aplicación de software que pretende ser un servidor en internet que no cuenta con ningún mecanismo ni configuración de defensa en contra de intrusiones fraudulentas. Actúan como sistemas señuelo para los hackers debido a que son atractivos por facilidad de acceso. Entre más un honeypot es atacado por intrusiones maliciosas es más valioso por la cantidad de información que ha recopilado. Existen dos tipos básicos de honeypots:

- **De alta interacción:** Dan a los hackers un ambiente real para atacar.
- **De baja interacción:** Imitan los ambientes de producción por lo tanto proveen información más limitada.

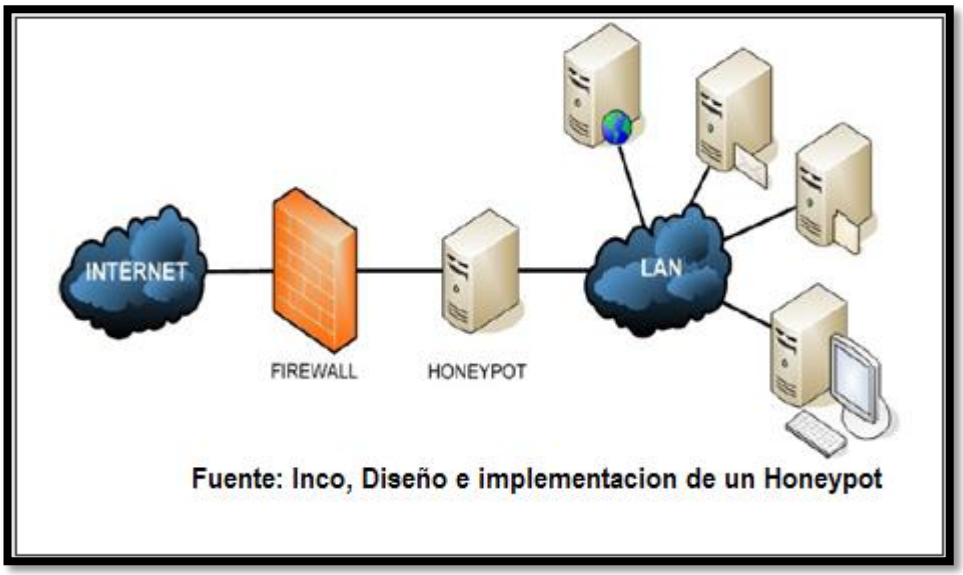


Figura 21: Implementación de un Honeypot detrás del firewall.
Fuente: http://honeypots.wordpress.com/2009/05/04/

Un honeynet es cuando existen múltiples honeypots en una red que simulan una arquitectura más grande. Al permitir a los hackers introducirse en la falsa red los atacantes dejan información de cómo llevaron a cabo la intrusión la cual es capturada con tecnologías de vigilancia.

Todo el tráfico tanto en un honeypot como en las honeynets se asume que es sospechoso, porque los sistemas no están destinados precisamente para ser atacados y recopilar información sobre ataques así puede actuar proactivamente al actualizar las vulnerabilidades de la red en producción en una organización.

Si un honeypot está diseñado para ser accesible desde la Internet, hay riesgo de que los servicios de monitoreo externo que crean listas de sitios no confiables puedan reportar al sistema de la organización como vulnerable, sin saber que las vulnerabilidades pertenecen al honeypot y no al sistema mismo. Dichas revisiones independientes hechas públicas pueden afectar la reputación de la organización. Por lo tanto antes de implementar un honeypot en la red se debe ejercer un juicio cuidadoso.

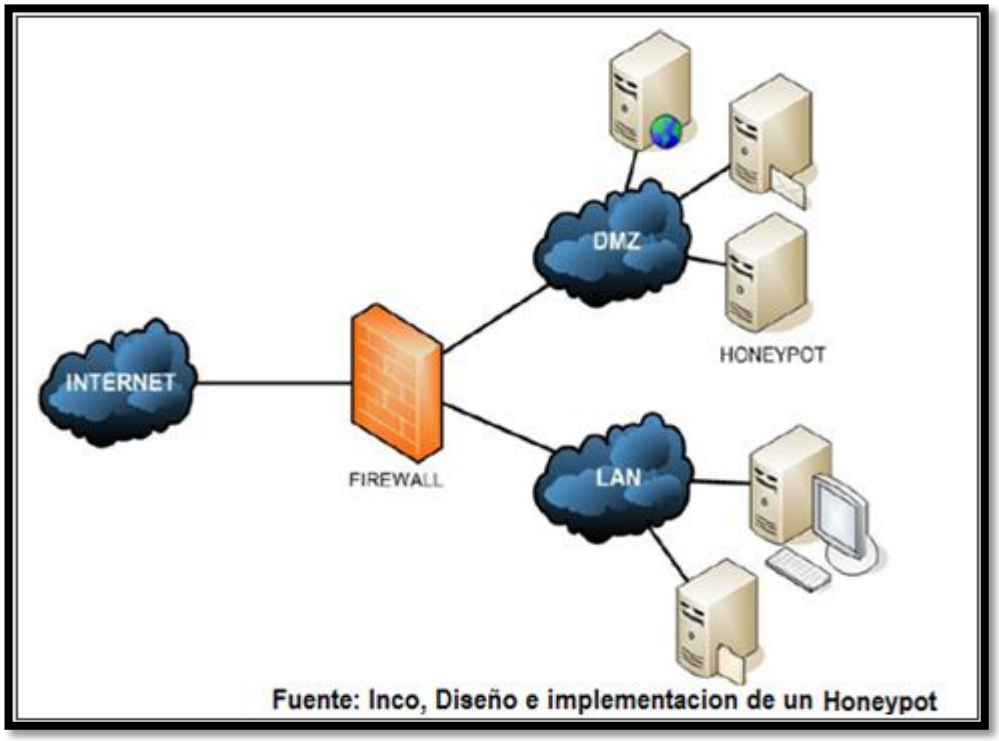


Figura 22: Implementación de Honeypot en una zona desmilitarizada.
Fuente: http://honeypots.wordpress.com/2009/05/04/

1.6 Reportes de Seguridad.

Para un administrador de red con conciencia sobre la importancia de la seguridad. La información proveniente de sitios autorizados como el de Microsoft, es de gran interés, porque ayudan en la prevención de posibles problemas de seguridad proveyendo de herramientas, pasos a soluciones, tendencias futuras de infección, sistemas operativos más vulnerables, etc. Se tomara como base los reportes de seguridad de Microsoft debido provee de gran cantidad de información gratuita y por la masiva utilización del sistema operativo Windows XP utilizado en entornos corporativos y educativos. Entre los reportes más relevantes están los siguientes:

- Boletines de seguridad
- Informes de Inteligencia de seguridad.

1.6.1 Boletines de seguridad.

Los boletines de seguridad proporcionados por Microsoft presentan información desde el año 2003 y es actualizado mensualmente. El mismo provee información como:

- Resumen Ejecutivo.
- Ubicaciones de descarga y software afectado
- Herramientas y consejos para la detección e implementación
- Información adicional

Resumen Ejecutivo: Se listan los Boletines por orden de gravedad. Donde se incluye información del boletín como: nivel de clasificación, si se requiere reinicio y el software afectado.

Ubicaciones de descarga y software afectado: Esta información es muy importante debido a que presentan las actualizaciones de seguridad desarrolladas y la importancia de

su instalación, los requisitos. Las cuales son desplegadas según la versión del sistema operativo.

Herramientas y consejos de detección e implementación: Probé vínculos donde podemos encontrar información más en concreto acerca de seguridad, consejos de detección e implementación, herramientas para detección de actualizaciones de seguridad en las estaciones de la organización, la importancia de utilizar un repositorio de actualizaciones como el Windows Server Update Servies WSUS y evaluadores de combatividad de aplicaciones.

Información adicional: Proporciona herramientas de eliminación de software malintencionado, estrategias de seguridad y enlaces a comunidades o foros donde se puede encontrar guías con la utilización de bases de conocimiento de la comunidad.

1.6.2 Informe de inteligencia de seguridad de Microsoft

Generados desde junio del 2006 los informes proporcionan una perspectiva en profundidad acerca del software malintencionado y potencialmente no deseado, vulnerabilidades de seguridad del software, infracciones de seguridad y vulnerabilidades de software (Importante indicar que no solo se proporciona información de software Microsoft sino también de terceros). En el volumen 7 del informe de inteligencia de seguridad (SIR siglas en inglés) Microsoft ha desarrollado perspectivas en base de un análisis de los últimos años, tomando con especial atención el primer semestre de 2009 (1M09). Entre los puntos más importantes del informe sobre el software malintencionado y potencialmente no deseado:

Tendencias geográficas

Los productos de seguridad de Microsoft reúnen, con el consentimiento del usuario datos de millones de equipos en todo el mundo y algunos servicios en línea con mayor actividad de

Internet. El análisis de estos datos proporciona una perspectiva completa y de la actividad relacionada con el malware y el software potencialmente no deseado en todo el mundo.

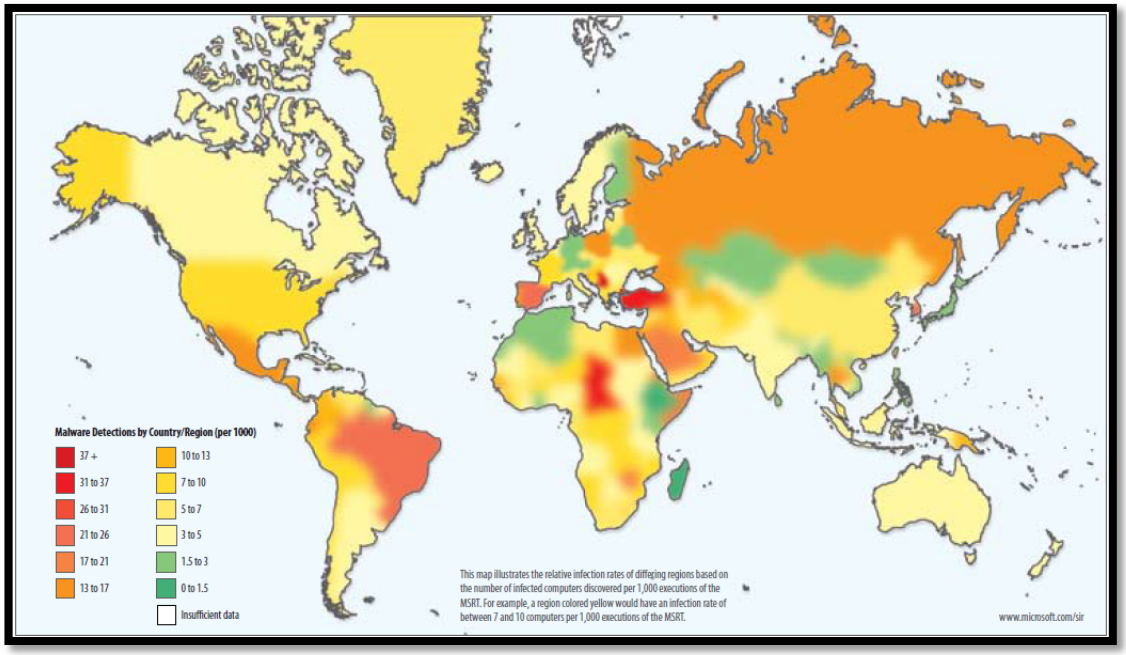


Figura 23: Tasas de infección por país/región durante el primer semestre de 2009 (expresado en número de equipos limpiados por cada mil)2.
Fuente: www.Microsoft.com/sir

En los Estados Unidos, el Reino Unido, Francia e Italia, los troyanos constituyeron la categoría principal de amenaza; en China, prevalecieron amenazas de diversos tipos principalmente basadas en los exploradores y en Brasil, fue más generalizado el malware contra la banca en línea.

Finalmente, en España y Corea, se generalizaron los ataques de gusanos con características de ataques en línea.

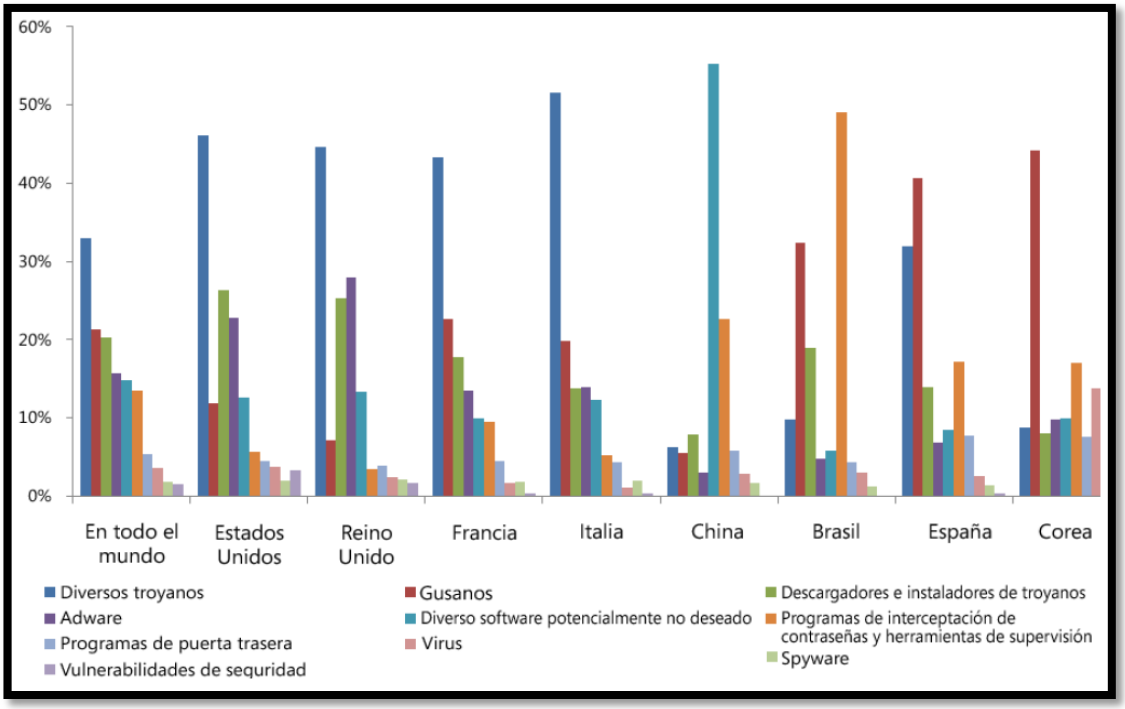


Figura 24: Categorías de amenaza de todo el mundo y en las ocho ubicaciones con el mayor número de equipos limpiados, organizadas por incidencias entre los equipos limpiados en el primer semestre de 2009.
Fuente: www.Microsoft.com/sir

Tendencias de los sistemas operativos

Debido a las diferentes versiones del sistema operativo de Microsoft Windows las cuales manejan diferentes niveles de control de seguridad se puede ver reflejado distintas tasas de infección, debido a las características y los Service Packs instalados con diversas versiones, así como las diferencias en la forma en que los usuarios y las organizaciones usan cada versión.

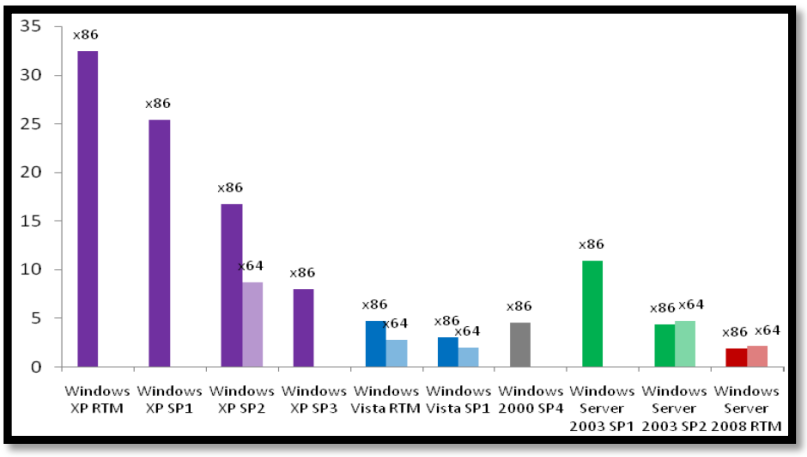


Figura 25: Número de equipos limpiados por cada 1.000 ejecuciones de la herramienta MSRT, organizados por sistema operativo, en el primer semestre de 2009.
Fuente: www.Microsoft.com/sir

Tendencias de Malware tratado en todo el mundo

- Diversos troyanos constituyeron la categoría más frecuente.
- Los gusanos pasaron del quinto puesto en el segundo semestre de 2008 a ser la segunda categoría más frecuente en el primer semestre de 2009.
- También se incrementó la presencia de programas de interceptación de contraseñas y herramientas de supervisión, debido en parte al aumento de malware contra jugadores en línea.

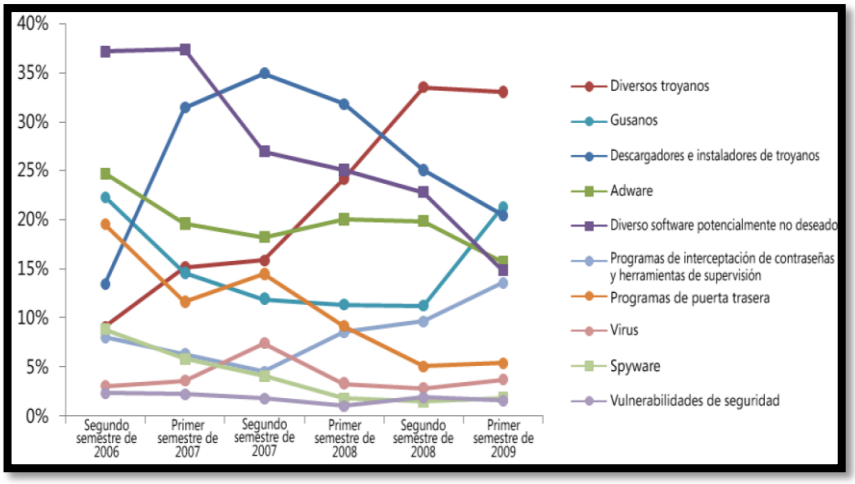


Figura 26: Porcentajes de equipos limpiados por categoría de amenaza del segundo semestre de 2006 al primer semestre de 2009. **Fuente:** www.Microsoft.com/sir

Distribución geográfica de los sitios que hospedan malware

- Al día se detectan más sitios de distribución de malware que sitios de suplantación de identidad (phishing).
- El hospedaje de malware tiende a ser más estable y menos diverso en términos geográficos.
- Esto se debe probablemente al uso relativamente reciente de las desconexiones de los servidores y la reputación de la web como armas contra la distribución de malware, lo que significa que los distribuidores de malware no se han visto forzados a diversificar su organización del hospedaje, al contrario que los suplantadores de identidad.

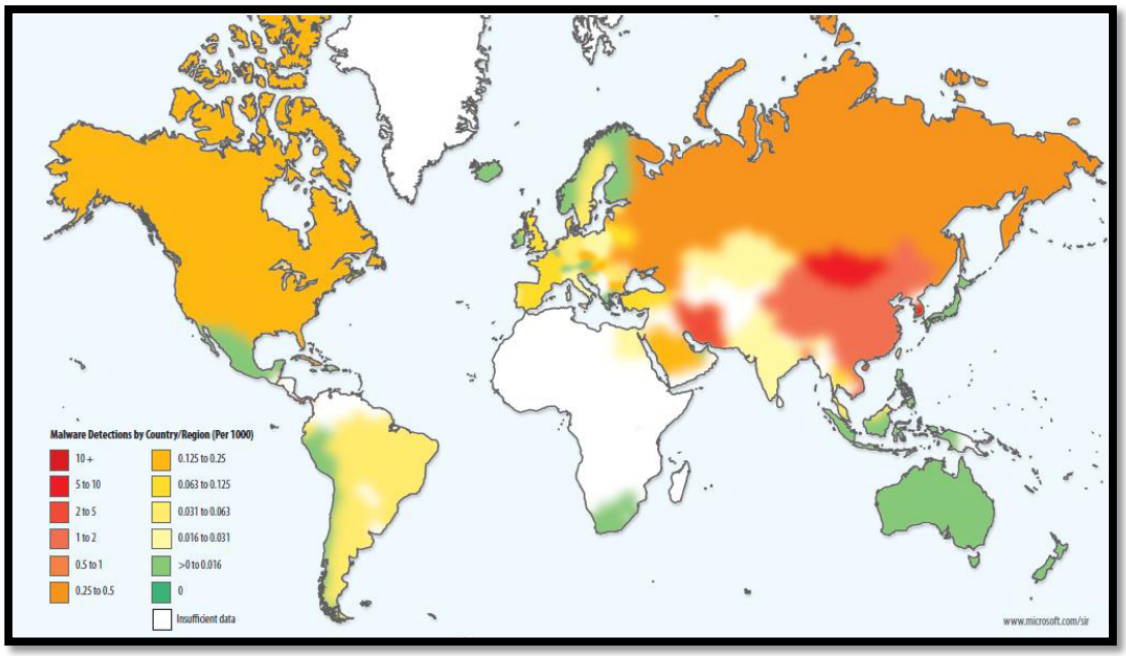


Figura 27: Sitios de distribución de malware por cada 1.000 hosts de Internet en ubicaciones de todo el mundo durante el primer semestre de 2009
Fuente: www.Microsoft.com/sir

Distribución geográfica de los sitios de suplantación de identidad (phishing)

Los sitios de suplantación de identidad (phishing) están hospedados en todo el mundo en sitios de hospedaje gratuito, en servidores web en riesgo y en otros muchos contextos. La realización de búsquedas geográficas de las direcciones IP de los sitios permite crear mapas que muestran la distribución geográfica de los sitios y analizar los patrones.

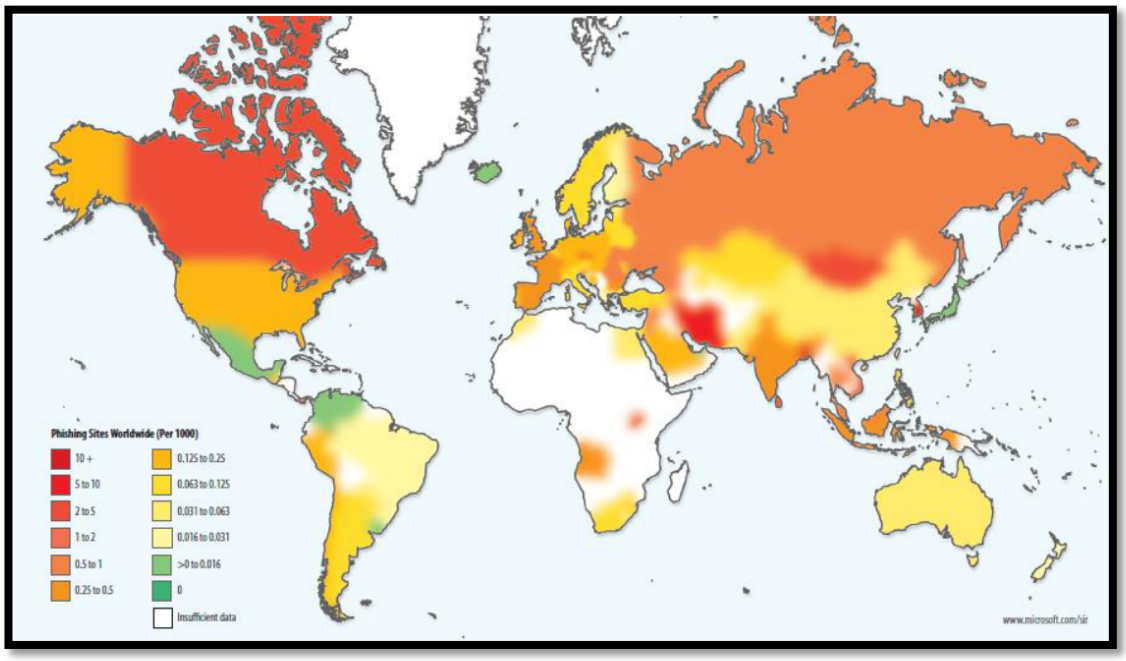


Figura 28: Sitios de suplantación de identidad (phishing) por cada 1.000 hosts de Internet en ubicaciones de todo el mundo en el primer semestre de 2009
Fuente: www.Microsoft.com/sir

Tendencias de las vulnerabilidades de seguridad: vulnerabilidades de seguridad basadas en explorador

Para evaluar el relativo predominio de las vulnerabilidades de seguridad basadas en explorador durante el primer semestre de 2009, Microsoft analizó una muestra de datos a partir de incidentes indicados por los clientes, envíos de código malintencionado e informes de errores de Microsoft Windows. Los datos abarcan diversos sistemas operativos y versiones de explorador, desde Windows XP hasta Windows Vista. Asimismo, se incluyen

datos de exploradores de terceros que hospedan el motor de representación de Internet Explorer, denominado Trident.

- En el caso de los ataques basados en explorador en equipos con Windows XP, las vulnerabilidades de Microsoft constituyeron el 56,4% del total. En los equipos con Windows Vista, las vulnerabilidades de Microsoft constituyeron sólo el 15,5% del total.

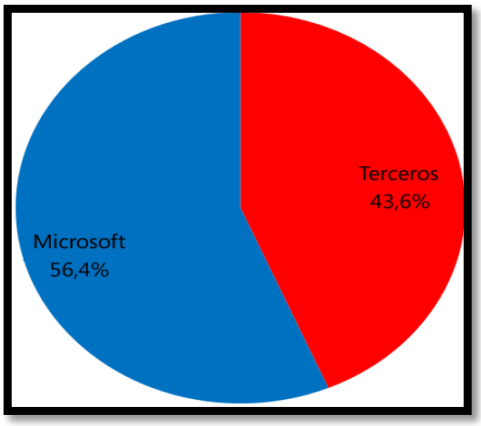


Figura 29: Vulnerabilidades de seguridad basadas en explorador dirigidas al software de Microsoft y de terceros en equipos con Windows XP durante el primer semestre de 2009
Fuente: www.Microsoft.com/sir

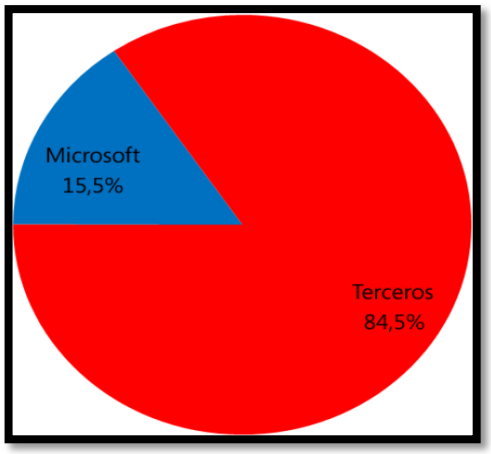


Figura 30: Vulnerabilidades de seguridad basadas en explorador dirigidas al software de Microsoft y de terceros en equipos con Windows Vista durante el primer semestre de 2009
Fuente: www.Microsoft.com/sir

El software de Microsoft presentó seis de las diez principales vulnerabilidades basadas en web en equipos con Windows XP durante el primer semestre de 2009, en comparación a sólo una en los equipos con Windows Vista. A continuación, se hace referencia a las vulnerabilidades según el número de boletín correspondiente del sistema de puntuación de vulnerabilidades comunes o del número del boletín de seguridad de Microsoft apropiado.

Análisis de las páginas de descarga no autorizada

- La mayoría de las páginas de descarga no autorizada están hospedadas en sitios web legítimos en riesgo. Los atacantes obtienen acceso a los sitios legítimos a través de intrusiones o mediante la publicación de código malintencionado en un formulario web poco protegido, como un campo de comentarios en un blog.
- Los servidores en riesgo que actúan como servidores de vulnerabilidades de seguridad pueden tener un alcance masivo: un servidor de vulnerabilidades de seguridad puede ser responsable de cientos de miles de páginas web infectadas.
- Los servidores de vulnerabilidades de seguridad en 2009 lograron infectar miles y miles de páginas en un breve período de tiempo.

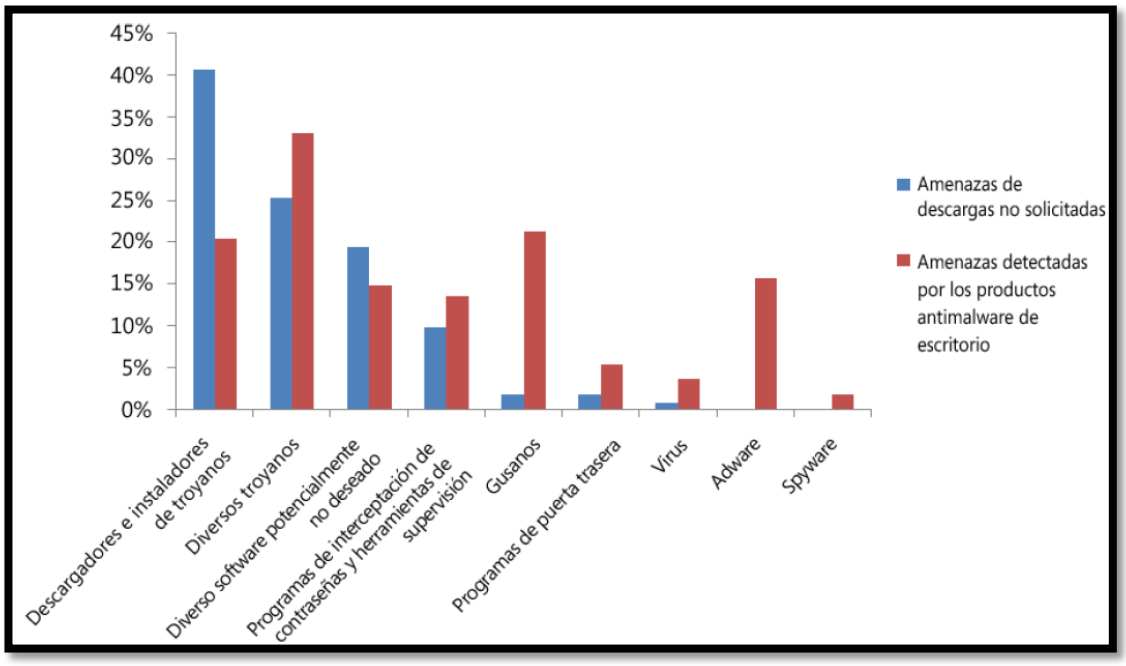


Figura 31: Tipos de cargas de amenazas transmitidas a través de descargas no autorizadas en el primer semestre de 2009
Fuente: www.Microsoft.com/sir

- La categoría de descargadores e instaladores de troyanos fue la más frecuente entre los sitios de descarga no autorizada con el 40,7%. Los descargadores de troyanos están preparados para su transmisión a través de descargas no autorizadas, ya que se pueden usar para instalar otras amenazas en los equipos infectados.

Capítulo 2: Soluciones de Seguridad.

La seguridad en una organización no solo depende de una solo, solución de seguridad que mantiene la red segura. Las soluciones de seguridad deben estar íntimamente relacionadas para evitar que los ataques maliciosos encuentren agujeros por donde ingresar a la red de la organización.

Siempre que un administrador u empresa contratada implementar un nuevo sistema de seguridad debe realizar un estudio de soluciones se encuentran ya implementadas para

determinar si las mismas pueden comunicarse o pueden complementarse a nivel total o parcial. Así con un conocimiento tanto de las nuevas tecnologías a implantarse como las existentes ayudaran a determinar cuáles son las mejores decisiones a tomar el momento de adquirir una solución misma que pueda cumplir con las necesidades de la organización de acuerdo a su presupuesto.

2.1 Tecnologías antimalware

Existen gran variedad de tecnologías antimalware provenientes de muchos proveedores que ofrecen una gama de servicios que van desde los gratuitos, online, pagados tanto para computadores de casa y soluciones empresariales. Todas estas tecnologías protegen a los pc contra el malware pero se tiene que considerar los escenarios donde se los va a utilizar ya que cada una tiene su respectiva aplicación que debería ser analizada antes de adquirir cualquiera de estos servicios.

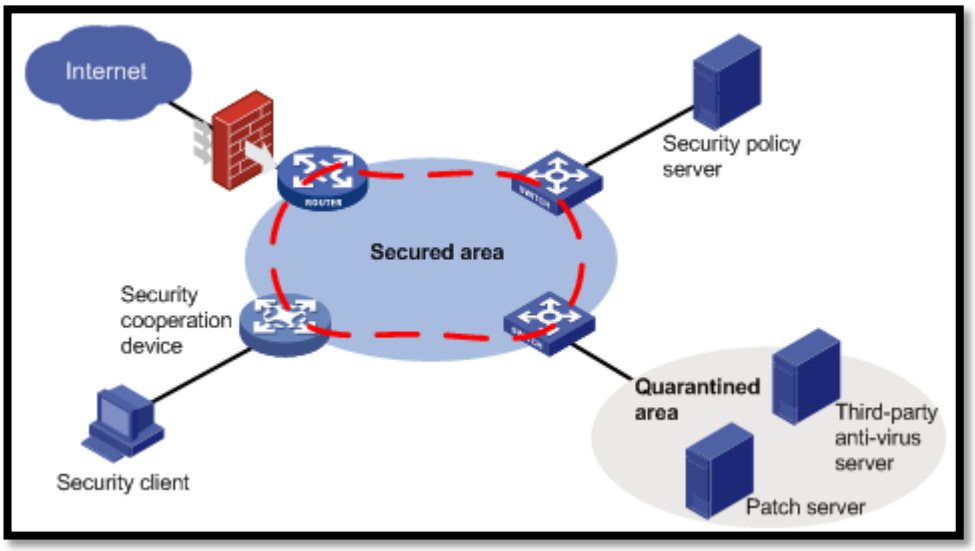


Figura 32: Topología de protección antivirus.
Fuente: http://www.h3c.com/portal/Products___Solutions

2.1.1 Controles Gerenciales de virus.

Lo primero que se debe tener presente antes de realizar cualquier instalación de software antivirus es manejar políticas y procedimientos tanto técnicos como administrativos, porque

el éxito para tener una red segura es tenerlas debidamente aseguradas desde el principio para evitar problemas más graves a futuro. Entre los controles y procedimientos a utilizar están:

- Instalar todo sistema a partir de copias maestras limpias (En lo posible proporcionadas por el fabricante) que estén debidamente vacunadas. Si se va a utilizar discos de inicio es preferible que estos sean originales y que los mismos tengan protección contra escritura.
- No permitir que se use ningún disco de instalación hasta que haya sido escaneado en una maquina independiente que no se use para ningún otro propósito y que no esté conectada en la red.
- Si se permiten demostraciones de proveedores, las mismas se deben pedir que sean realizadas en computadores de su propiedad.
- Aunque el software libre reduce costos, es mejor manejar la norma de no utilizarlos o manejarlos sin ningún control los instaladores deben ser antes debidamente probados y escaneados para evitar ser contagiados si los programas tienen algún tipo de código malicioso.
- Asegurar que las actualizaciones a utilizar para computadores o cualquier otro periférico como Firewalls y Gateways, sean descargados de lugares seguros y de propiedad de la marca.
- Los respaldos son de vital importancia un plan debe ser implementado para realizar las respectivas copias de seguridad. Este plan debe encargarse de escanear en lo posible los archivos más importantes en busca de infecciones de virus para evitar tener copias de seguridad infectadas.
- La educación al usuario es parte fundamental para manejar un buen nivel de seguridad en la red para que tenga presente las políticas y procedimientos.

Por ejemplo: Indicarles que muchos virus son propagados mediante los adjuntos de los correos electrónicos los cuales infectan las estaciones de trabajo al abrirlos. Indicar las técnicas de ingeniería social utilizadas por los hackers para hacer que los usuarios abran los adjuntos.

- Revisar las políticas y procedimientos por al menos una vez al año para evitar que las mismas queden caducas.
- Preparar un procedimiento de erradicación de virus e identificar los principales puntos de infección así como el personal que más incurre en esta falta, para indicar a la persona encargada el problema con el usuario es recurrente.

2.1.2 Controles técnicos

Se pueden implementar métodos de prevención de virus a través de medios de hardware y software. Entre las técnicas que podemos utilizar a nivel de hardware están:

- Protección de virus de reinicio (Boot) Ejemplo: Protección contra virus basada en Firmware integrado.
- Configurar contraseñas en el BIOS
- En el BIOS deshabilitar el Boot mediante unidades de disquete, CD o DVD ROM o unidades extraíbles USB.
- Asegurar que los todas las configuraciones del firewall estén funcionando como bloquear acceso a sitios inseguros de internet.

Sin embargo, el software es la herramienta comúnmente utilizada y se le considera el medio más efectivo de protección de las redes y sistemas usado como un control preventivo.

El software antivirus contiene un número de componentes que se ocupan de la detección de virus mediante las tecnologías escaneo desde diferentes ángulos de donde podría provenir un ataque. Pero los dos principales son Mascaras o firmas de virus y Escáneres heurísticos.

- **Mascaras o firmas de virus:** El antivirus escanea la memoria y sectores del disco duro conocidos donde siempre se alojá los virus. Utilizando como base las máscaras o firmas de virus descargadas de internet para determinar si existe código malicioso ejecutándose. Las máscaras o firmas son cadenas de código específico que son reconocidas como pertenecientes a un virus. Pero debido a que también existen virus polimórficos el software antivirus poseen algoritmos diseñados por cada fabricante para verificar si hay posibles variaciones de virus para detectarlos.
- **Escáneres heurísticos:** Trabajan analizando las instrucciones en el código de programas que determina con comportamiento extraño decidiendo si podría contener código malicioso, esto lo hace en base de probabilidades estadísticas. Los resultados de un escaneo heurístico pueden indicar presencia de virus así no se tenga firmas actualizadas o si es un nuevo virus del cual no existe todavía cura o firmas para detenerlo. Los escáneres heurísticos tienden a generar un alto nivel de errores de falsos positivos es decir presencia de virus cuando no existe.

2.1.3 Estrategia de implementación de Software Antivirus

Las organizaciones tienen que desarrollar estrategias de implementación de antivirus para controlar y prevenir efectivamente la propagación de virus a través de todos los sistemas de la red y no solamente instalarla en todas las estaciones esperando que arregle automáticamente todos nuestros problemas de virus.

Un mecanismo importante para controlar la propagación de virus es detectar los puntos más vulnerables en la organización es decir donde tienen más posibilidad de encontrar sistemas a infectar y mantener un mayor control de los mismos. Pero estrategias similares deben desarrollarse para todas las estaciones de la red. La plataforma antivirus a ser utilizada en servidores y estaciones de trabajo debería manejar controles como:

- Escaneos programados de virus (diarios, semanales, etc)

- Escaneos manuales a petición, donde pueda ser realizado por el administrador o por los usuarios con ciertas restricciones.
- Escaneo continuo (real-time-protection), donde cualquier dispositivo que sea conectado al computador sea escaneado inmediatamente así el usuario no lo solicite y realice escaneos continuos tanto de sectores delicados así como de archivos importantes del sistema.

A nivel de una red corporativa el software antivirus se encuentra en colaboración con tecnologías que verifican el tráfico de la red como firewalls. El firewall es la primera muralla contra los virus ya que escanean el tráfico entrante y saliente con la intención detectar, eliminar acceso a sitios con potencial código malicioso, etc. Entre los niveles de seguridad se incluyen:

- Protección SMTP, para escanear el trafico SMTP entrante y saliente, detectando virus en coordinación con el servicio de correo.
- Protección HTTP, para prevenir que los archivos infectados con virus sean descargados y ofrecer protección contra código malicioso ejecutable en las páginas como Java y ActiveX.
- Protección FTP, para prevenir ingresos no autorizados e impedir acceso de archivos infectados.

Un firewall configurado en la red no garantiza que todos los virus sean excluidos efectivamente de ahí la importancia de coordinar la protección con el software antivirus el cual tiene mayor facilidad de actualizar sus firmas en contra de nuevas amenazas que se detectan diariamente. Pero todo software antivirus para que tenga un nivel aceptable de protección debe tener entre sus características de escaneo:

- **Confiabilidad y calidad:** En la detección de virus.

- **Residente en memoria:** Funcionalidades de verificación continúa.
- **Eficiencia:** En consumo de recursos y velocidad de respuesta ante posibles contagios.

2.2 Sistemas de Seguridad Firewall (contrafuegos)

Cuando una empresa conecta su infraestructura de red interna a Internet se enfrenta instantáneamente a peligros potenciales debido a las características de Internet.

Toda red corporativa conectada a internet es vulnerable a un ataque asi los hackers en Internet podrían teóricamente introducirse a la red corporativa y hacer daño de muchas formas como: hurtar o dañar datos sensibles, dañar computadoras personales, servidores es decir afectar a toda la red. Esa posibilidad se da al tener acceso a los recursos corporativos de la red. Las empresas deben establecer los firewalls como un medio de seguridad perimetral para sus redes. Este principio debería ser aplicado incluso para sistemas sensitivos o importantes que necesitan ser protegidos de usuarios internos de la red corporativa.

Los firewalls se definen como un dispositivo instalado en el punto donde las conexiones de la red entran a un lugar que aplica reglas para controlar el tipo de tráfico de red que fluye hacia adentro y hacia afuera. La mayoría de los firewalls comerciales están elaborados para manejar protocolos relacionados con el uso de Internet.

Para ser efectivos, los firewalls deben permitir a las persona que están en la red corporativa entrar a Internet y al mismo tiempo deben impedir a los intrusos o a otros en internet ganar acceso a la red corporativa para ocasionar daños.

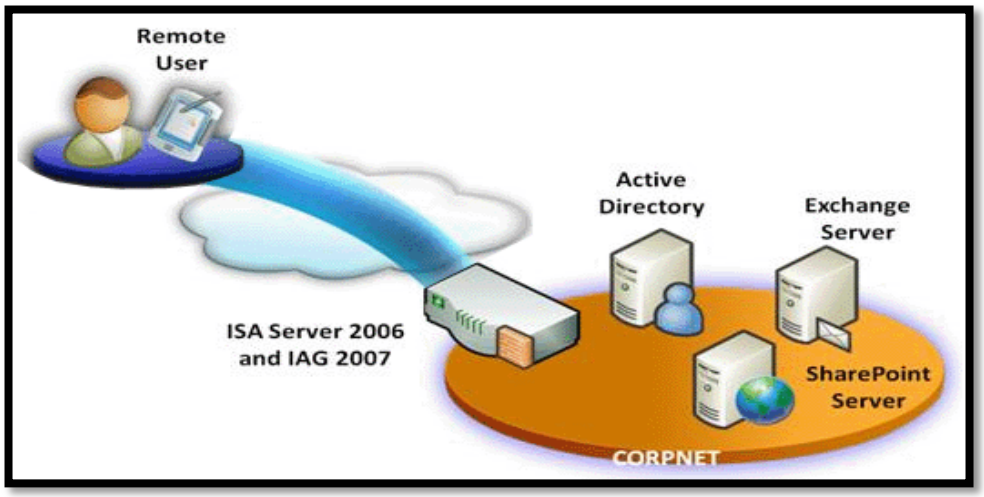


Figura 33: Topología de protección firewall básica software Microsoft producto ISA server 2006.
Fuente: http://www.microsoft.com/forefront/edgesecurity/isaserver.

2.2.1 Características Generales de los firewalls

Los firewall son combinaciones de hardware y de software o solo software. Deben ubicarse en el punto más vulnerable que generalmente esta entre una red corporativa e internet y pueden ser tan sencillos o tan complejos como lo exija la política corporativa de seguridad de la empresa o de los recursos que se disponga. Aunque existen muchos tipos de firewalls la mayoría de ellos deberían permitir controles como:

- Bloquear el acceso a sitios particulares en Internet
- Limitar el tráfico en el segmento a segmentos de la red controlando accesos a servicios, direcciones y puertos sensibles.
- Impedir que determinados usuarios tengan acceso a ciertos servidores.
- Monitorear las comunicaciones entre la red interna y una red externa.
- Monitorear, grabar todas las comunicaciones entre una red interna y el mundo exterior para investigar y tener pruebas de auditoria de ser necesarias.
- Encriptar / Cifrar paquetes que son enviados entre diferentes ubicaciones físicas dentro de una organización creando una red privada virtual en Internet.

Se pueden extender las funcionalidades de algunos firewalls de modo que puedan también proporcionar protección contra los virus y ataques dirigidos a explotar las vulnerabilidades conocidas del sistema operativo.

2.2.2 Problemas del firewall

Los problemas que enfrentan las organizaciones que han implementado firewalls incluyen:

- Existe un falso sentido de seguridad cuando la administración siente que no se necesitan más verificaciones y controles de seguridad en la red interna (es decir, la mayoría de los incidentes son ocasionados por agentes internos, que no son controlados por los firewalls).
- Los firewalls son burlados por medio del uso de módems que conectan a los usuarios directamente con los proveedores de servicios de internet. La gerencia debe proveer garantías de que el uso de los modem cuando existe un firewall este estrictamente controlado o prohibido totalmente.
- Firewalls mal configurados que permiten que servicios desconocidos y peligrosos pasen libremente.
- La interpretación equivocada de que es lo que constituya un Firewall (por ejemplo, las compañías que sostienen que tienen un Firewall tienen meramente un enrutador filtrante).
- Las actividades de monitoreo no se llevan a cabo periódicamente (es decir, las disposiciones de registro no se aplican y revisan de manera apropiada).
- Las políticas de Firewall no se mantienen periódicamente.
- La mayoría de Firewalls operan en la capa de red, por lo tanto, no pueden parar ataques basados en aplicaciones o entradas (inputs). Los ejemplos de estos ataques incluyen ataques de SQL inyección o desbordamiento de buffer. La

generación de Firewalls más reciente son capaces de inspeccionar el tráfico a nivel de la capa de aplicación y parar algunos de estos ataques.

2.2.3 Plataformas Firewall

Los firewall pueden ser implementados usando plataformas de hardware o de software. Cuando se implementan en hardware se obtiene un buen rendimiento con un nivel de sobrecarga mínima. A pesar de que los firewalls basados en hardware son más veloces, no son tan flexibles ni escalables como los basados en software.

Los firewalls basados en software son generalmente más lentos y generan sobrecarga en los sistemas; sin embargo, son flexibles porque pueden utilizar servicios adicionales. Pueden incluir verificación de contenido y de virus antes de que trafico sea pasado a los usuarios.

Generalmente es mejor usar equipo especializado (appliance), en lugar de servidores convencionales para los firewalls. El hardware especializado es normalmente instalado con sistemas operativos reforzados. Cuando se usan firewalls basados en servidores, los sistemas operativos en los servidores son a menudo vulnerables a ataques. Cuando los ataques a los sistemas operativos tienen éxito, el firewall se vería comprometido. Los firewalls basados en hardware especializado (appliances) son, por lo general, considerablemente más veloces de establecer y de recuperar.

2.2.4 Sistemas de detección de intrusos IDS.

Otro elemento para asegurar las redes que complementa las implementaciones de Firewall es un sistema de detección de intrusos (IDS). Los IDS's funcionan en conjunto con los enrutadores y con los firewalls monitoreando las anomalías en el uso de la red. Protege los recursos de los sistemas de información de una compañía tanto de ataques maliciosos externos como internos.

Un IDS opera de manera continua en el sistema, corriendo en el background (sin afectar al desarrollo normal del sistema) y notificando a los administradores cuando detecta una amenaza. Entre las categorías de los IDSs se incluyen:

- **IDS basados en la red:** Estos identifican los ataques dentro de la red que están monitoreando y emiten una advertencia al operador. Si un IDS basado en la red se coloca entre la Internet y el Firewall, detectara todos los intentos de ataque, tanto del tráfico que paso el firewall como los que no pasaron el firewall. Si el IDS es colocado entre un Firewall y la red corporativa, detectara los ataques que pudieron evitar el firewall (detectara intrusos). Pero se debe tener en cuenta que el IDS no es un sustito del firewall sino que complementa la función de un firewall.
- **IDS basados en un host:** Están configurados para un ambiente especifico y monitorean los distintos recursos internos del sistema operativo para advertir sobre un posible ataque. Ellos pueden detectar la modificación de los programas ejecutables, la eliminación de archivos y pueden emitir una advertencia cuando se hace un intento de usar un comando privilegiado.

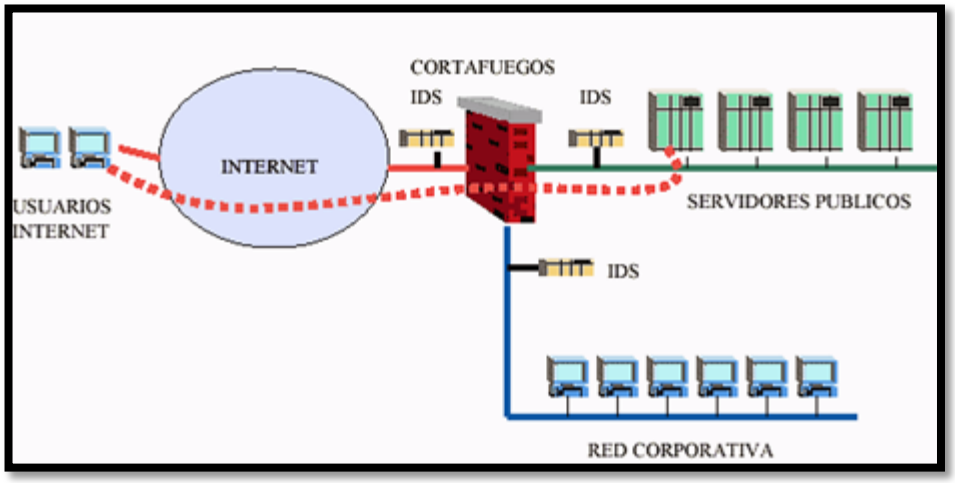


Figura 34: Topología de protección IDS.
Fuente: http://www.windowsecurity.com/articles/Keeping_IDS_InHouse.html.

Los componentes de un IDS son:

- Los sensores que son responsables de la recolección de los datos. Los datos pueden estar en la forma de paquetes de red, archivos de registro, trazas de llamada de sistema, etc
- Los analizadores reciben información proveniente de los sensores y determinan la actividad de intrusos.
- Una consola de administración.
- Un interfaz de usuario.

Los tipos de IDS incluyen:

- **IDS basados en firma:** Estos sistemas de IDS protegen contra los patrones de intrusos detectados. Los patrones de intrusos que pueden identificar son almacenados en forma de firmas.
- **IDS basados en estadísticas:** Estos sistemas necesitan una definición detallada del comportamiento conocido y esperado de los sistemas.
- **Redes neuronales:** Un IDS que tiene esta característica monitorea los patrones generales de la actividad y de tráfico en la red creando una base de datos sobre los comportamientos de la red. Esto es similar al modelo estadístico pero con funcionalidad agregada de auto-aprendizaje.

Los IDSs basados en firma no podrán detectar todos los tipos de intrusos debido a las limitaciones de las reglas de detección. Por otra parte los sistemas basados en estadísticas pueden reportar muchos eventos fuera de la actividad normal definida pero que son actividades normales en la red. Una combinación de modelos basados en firma y basados en estadísticas provee una mejor protección.

Características

Las características existentes en un IDS incluyen:

- Detección de intrusos.
- Recolección de evidencias sobre actividad de intrusos.
- Respuesta automatizada (Terminación de la conexión, envió de mensajes de alarma).
- Políticas de seguridad.
- Interfaz con las herramientas del sistema.
- Administración / Gestión de las políticas de seguridad.

Limitaciones

Un IDS no puede ayudar con las debilidades siguientes:

- Debilidades en la definición de políticas.
- Vulnerabilidades en el nivel de aplicación.
- Puertas traseras en las aplicaciones.
- Debilidades en la identificación y en la autentificación.

En contraste con los IDS, que se basan en archivos de firma para identificar un ataque cuando o después de que ocurre, un sistema de prevención de intrusos (IPS) predice un ataque antes que pueda ocurrir. Hace esto monitoreando las áreas clave de un sistema de computador y busca "mal comportamiento" como por ejemplo: gusanos, troyanos, spyware, malware y hackers. Así los IDSs complementan las herramientas de firewall, antivirus y antispyware para proveer completa protección contra las amenazas emergentes diariamente.

2.3 Soluciones para Usuario Final.

El software antivirus conocido comúnmente es el utilizado en nuestros computadores propios los cuales nos permiten tener un control total de la plataforma antivirus, es decir podemos configurar y utilizar todos sus menús de configuración a nuestra conveniencia y la mayor parte de estas configuraciones quedan en estado por defecto. Aunque podemos realizar cualquier configuración los usuarios más experimentados o con conocimientos más avanzados sobre herramientas antivirus son quienes verdaderamente conocen para que son las opciones disponibles y pueden aprovechar la herramienta más que un usuario sin experiencia.

Las soluciones antivirus que utilizamos en nuestros computadores propietarios nos son siempre las seleccionadas de forma técnica ya que utilizamos las entregadas de forma gratuita al comprar el computador o por recomendaciones de las personas en nuestro entorno social quienes conocen de sistemas o simplemente están utilizando el software antivirus. Se podría afirmar que utilizar una solución antivirus cualquiera que esta sea es mejor que no tener ninguna pero se debería tener un mayor cuidado al adquirí cualquiera de las disponibles. Un antivirus debe ser evaluado por distintas características como:

- Su capacidad heurísticas en detección de virus sin firmas antivirus.
- Velocidad de escaneo y respuesta efectiva al detectar software antivirus.
- Buena capacidad de actualización contra nuevas amenazas.
- Efectividad al detectar virus en todas sus versiones futuras.
- Efectividad al eliminar virus y recuperar archivos infectados.
- Consumo mínimo de recursos al sistema.
- Menús de configuración accesibles y fáciles de utilizar tanto para expertos e inexpertos.
- Documentación accesible.

- Costo del software (Versiones gratuitas o con licenciamiento).

Ya que existen muchas variables a tomar a en cuenta antes de tomar la decisión del tipo de antivirus vamos a adquirir no es fácil tomar la decisión porque no todos son expertos en seguridad antivirus como para realizar los estudios necesarios y evaluar todas las características antes mencionadas, es así como organizaciones internacionales como "Virus Bulletin Fighting malware and spam" se encargan de realizar las respectivas evaluaciones de las marcas de software antivirus más conocidas a nivel mundial.

2.3.1 Virus Bulletin (VB).[7]

Virus Bulletin se convirtió en la principal publicación especialista en el campo de virus y malware relacionado, la cual comenzó en 1989 como una revista dedicada a proporcionar a los usuarios de PC una fuente regular de información acerca de: virus informáticos, su prevención, detección, eliminación y como recuperar información después de ataques de software malicioso.

Mantener la independencia ha sido siempre la principal preocupación de VB. Cortando de raíz cualquier promoción exagerada e influenciada por proveedores de software antivirus de cualquier marca. El principal objetivo de la revista es brindar a los usuarios la información necesaria para mantenerlos actualizados con las últimas novedades en el campo de anti-malware.

Durante muchos años, Virus Bulletin ha llevado a cabo pruebas comparativas independientes de productos antivirus, otorgando la certificación VB100 que es

[7] MARTIN, Helen, *Virus Bulletin about us* [en línea]. Virus Bulletin, 2010, [citado 1-2-2010], Disponible en Internet: http://www.virusbtn.com/about/index.

ampliamente reconocida en la industria de seguridad antivirus. A diferencia de otros sistemas de certificación, Virus Bulletin realiza pruebas de todos los productos en forma gratuita y no permite re-testing ni realizar modificaciones del software entregado ya que se realizan las pruebas de software exactamente como se encuentran a la venta al público en general. En 2009 se introdujo un nuevo concepto de pruebas anti-malware por parte de "Virus Bulletin", las bautizadas por la revista pruebas RAP donde se toma en cuenta las habilidades de detección heurística y capacidades de soluciones antimalware. Virus Bulletin utiliza la experiencia adquirida durante más de una década para realizar las pruebas comparativas de anti-malware de forma periódica e independiente.

2.3.2 Pruebas RAP.

La prueba mide las tasas de detección de los productos seleccionados mediante el uso de cuatro grupos de muestras distintas de malware. Los tres primeros grupos de malware de prueba son de las 3 semanas antes de que el producto haya sido entregado para su evaluación. Estos tres primeros grupos sirven para medir la rapidez con que los desarrolladores y laboratorios de los productos reaccionan ante la aparición de nuevo malware los cuales se propagan de forma increíblemente rápida todo el mundo diariamente. El cuarto conjunto de prueba consta de muestras de malware nuevo tomado después de la semana que fue entregado el producto para realizar las respectivas pruebas. Con este último conjunto se realizan pruebas para medir la capacidad de los productos para detectar nuevas y desconocidas versiones de virus, es decir esta prueba mide la capacidad de detección de los algoritmos heurísticos que poseen los productos antivirus.

2.3.3 Resultados de las pruebas RAP.

Los resultados de las pruebas son representados también gráficamente con gráficos de barras como las expuestas a continuación:

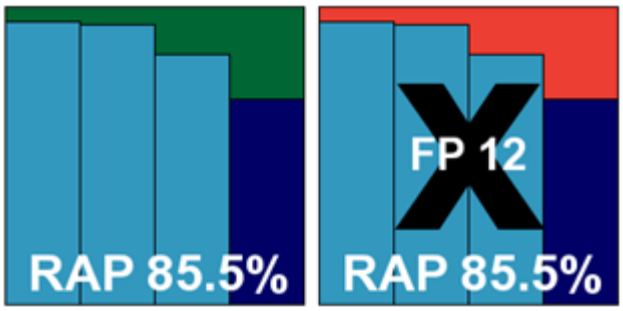


Figura 35: La figura derecha incida la aprobación de las evaluaciones de Virus Bulletin. La figura izquierda muestra el número de falsos positivos del producto evaluado e indica que no aprobó la certificación de Virus Bulletin.
Fuente: http://www.virusbtn.com/vb100/vb200902-RAP-tests

Las tres barras celestes representan las semanas -3, -2 y -1, mientras que la barra azul oscura representa semana + 1. La puntuación llamada 'RAP puntuación' también es presenta en el gráfico la cual representa el promedio de detección de todos los productos evaluados durante las cuatro semanas. En los casos donde los productos han generado falsos positivos en las pruebas se coloca al fondo del gráfico con colores rojo y una gran equis, junto a las letras ' FP = ' el número de falsos positivos generados. Esta indicación funciona como advertencia a los usuarios y lectores de "Virus Bulletin" para que conozcan cuales fueron los productos que no aprobaron las evaluaciones realizadas.

Resultados de la prueba de RAP de Virus Bulletin año 2009.

El siguiente gráfico muestra los resultados RAP obtenidos entre agosto de 2009 y de 2010 de febrero, la relación se la hace con las puntuaciones medias de los resultados reactivos (De las 3 primeras semanas) versus las puntuaciones medias de los resultados proactivos (Cuarta y última semana) de cada producto.

Los suscriptores del boletín de virus tienen acceso a los resultados detallados de las pruebas RAP e incluyen un cuadrante RAP por cada prueba realizada.

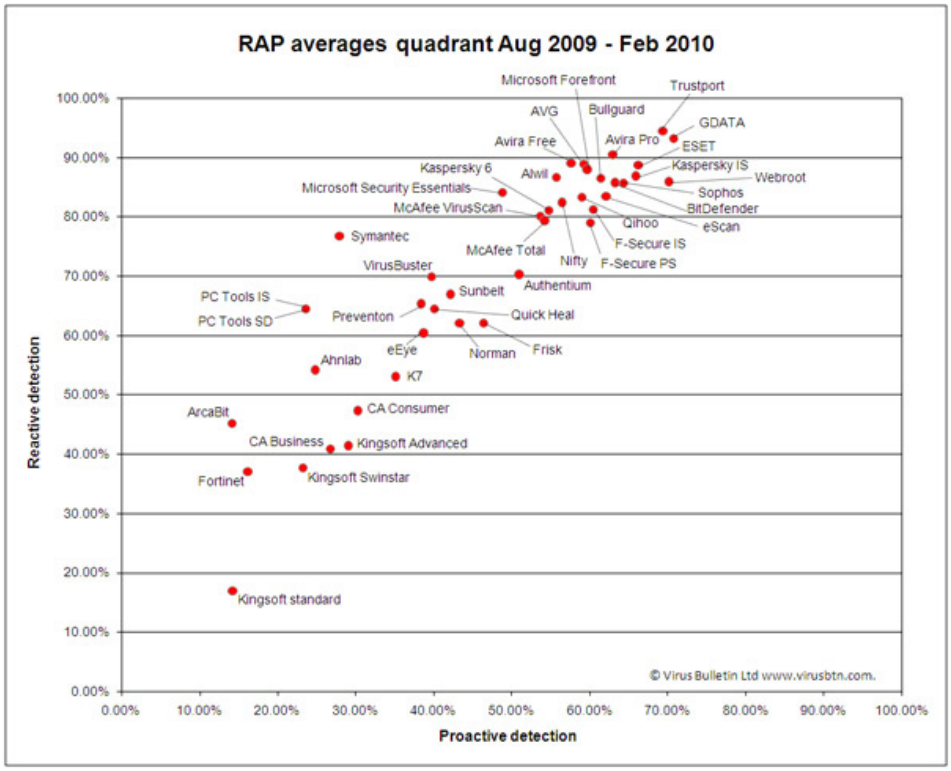


Figura 36: Cuadrante RAP periodo 2009 a Febrero 2010.
Fuente: http://www.virusbtn.com/vb100/rap-index.xml

2.4 Solucione Empresariales.

Las soluciones antivirus son importantes y mucho más en entornos empresariales donde protegen las herramientas de trabajo que son ahora las computadoras las cuales almacenan toda información, aplicaciones y son el medio de comunicación de la organización. Pero no se puede utilizar el mismo tipo de software que utilizamos de forma común en nuestros computadores propietarios porque el software que es diseñado para estas estaciones tiene una plataforma administrable similar a una isla es decir cualquier actualización, configuración, regla, etc. Solo es configurada para esa estación en específico y no puede replicarse en un entorno de red.

El problema no podría ser visible cuando manejamos entornos donde solo existen pocas estaciones de trabajo con fácil acceso en un solo piso u oficina. En estos entornos utilizar cualquier software antivirus inclusive de distintas marcas protege los computadores de

forma efectiva sin mayor complicación porque cada usuario es responsable de la seguridad de su estación en cierta forma.

Pero al manejar entornos donde existen un gran número de estaciones de trabajo no se podría dedicar el tiempo ni los recursos para monitorear a cada estación en persona observando si las mismas están actualizadas, ejecutando escaneos periódicos, configurando políticas e inclusive realizado la instalación ya que sería una tarea realmente exhaustiva.

Es así como los diseñados de software antivirus lanzaron soluciones específicas para entornos corporativos donde se utilizan servidores centralizados los cuales por medio de consolas graficas ofrecen estadísticas e informes de ataques recientes, focos de infección, estado de la seguridad, nivel de actualizaciones, en fin de acuerdo al software adquirido su consola entregara diversa información relacionada.

Lo más importante de utilizar un servidor central antivirus es proporcionar actualizaciones de las firmas de seguridad antivirus sin la necesidad de que todas las estaciones se conecten a internet directamente, ya que el servidor sirve de repositorio central donde todos las computadoras de la red se conectan así se evita el problema del congestionamiento del ancho de banda de internet.

Otro factor impórtate de la centralización es la posibilidad de configurar políticas a sus clientes de forma centralizada como por ejemplo las horas de actualización, escaneos programados a ciertas horas en modo (rápido-completo), acceso a los menús de configuración, etc. Prácticamente los usuarios pueden obviar la utilización de software antivirus aunque en su gran mayoría lo hace sin necesidad de indicárselo. Así cuando el administrador de la red configura las políticas en el servidor central las mismas se actualizan después de tiempos especificados o por defecto en todas las estaciones de la red, permitiendo al administrador estar seguro de que mantiene un nivel de seguridad eficaz con

un antivirus actualizado y que realiza escaneos periódicos sin intervención de los usuarios de las estaciones necesariamente.

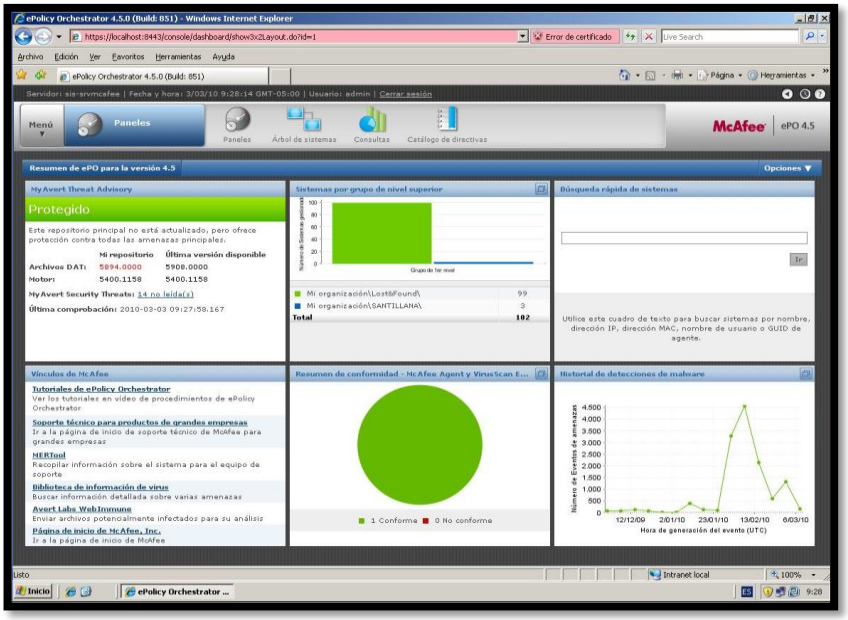


Figura 37: Consola central Mcafee 8.7.
Fuente: Hugo Paredes

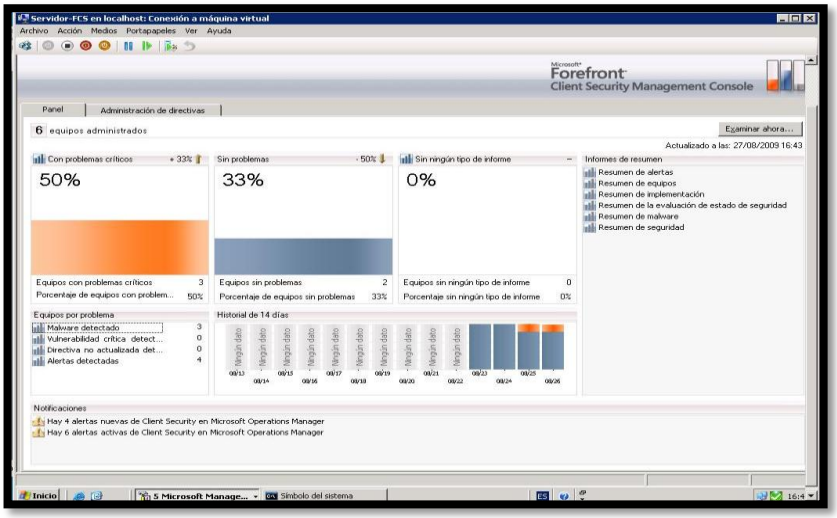


Figura 38: Consola central FCS.
Fuente: Hugo Paredes.

Existe otro servidor que debe ir de la mano con cualquier software antivirus centralizado es un repositorio centralizado de actualizaciones de seguridad de los sistemas operativos. Es de vital importancia implementar este tipo de servidores porque ayudan a mantener los

sistemas operativos de la red actualizados con las últimas versiones de seguridad ya que si recordamos los virus buscan atacar vulnerabilidades de los sistemas operativos y por más que se tenga funcionando el software antivirus con las ultimas firmas de antivirus. Cualquier virus que ataque vulnerabilidades no actualizadas tendrá camino libre para atacar y afectar a los computadores no actualizados en la red. Es una de las principales causas de las epidemias de virus a nivel mundial.

Un ejemplo de este tipo de repositorios centralizados es la consola gratuita de Microsoft la conocida como Windows Server Update Services (WSUS), la cual permite descargar actualizaciones de seguridad de todo el software de Microsoft tanto para sistemas operativos, aplicaciones de ofimática como office, actualizaciones de software antivirus Microsoft Forefront, entre otras.

Una vez que la consola es integrada a la red del directorio activo detecta a las computadoras de la red y mediante un escaneo indica su estado señalando cuales son las actualizaciones de seguridad que necesita cada computadora en particular. El estado de la actualización se muestra de forma gráfica o con porcentajes y el repositorio permite seleccionar cuales actualizaciones descargar y cuales instalar. Es decir se podría bajar los service pack 2 y 3. De Windows XP y decidir instalar un grupo de computadores con service pack 2 y otro grupo con service pack 3.

La gran ventaja de esta consola entre otras es que es gratuita se integra de forma nativa con el directorio activo de la organización lo cual permite mediante una directiva de grupo indicar que las actualizaciones de seguridad del sistema operativo se realicen de forma centralizada en el servidor WSUS y ya no mediante la conectividad al sitio de Microsoft Windows Update. Una vez más cuidando el ancho de banda de internet y facilitando la distribución de las actualizaciones de forma automática.

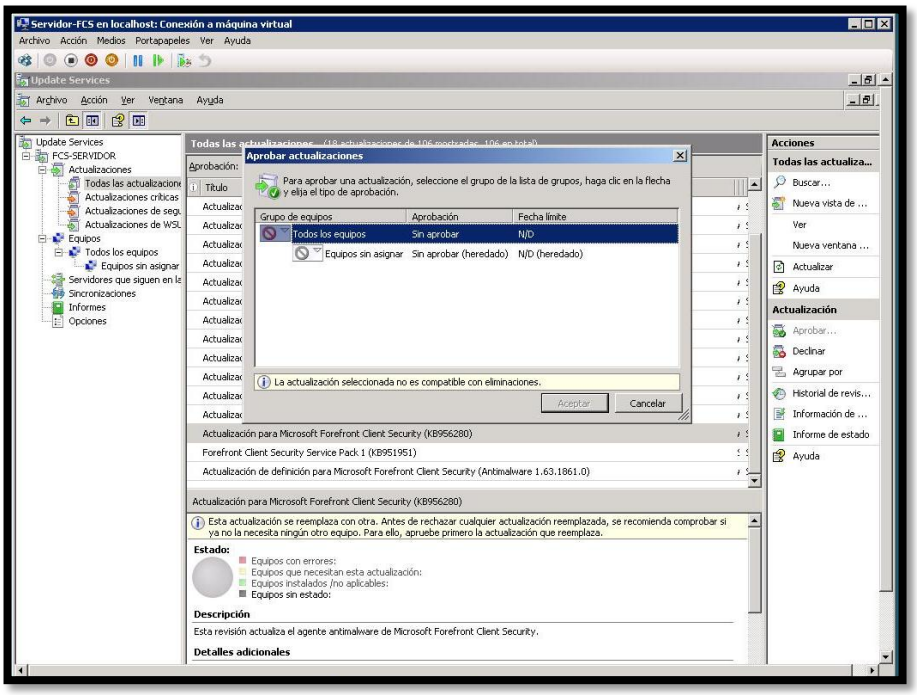


Figura 39: Consola central WSUS, aprobación de actualizaciones.

Capítulo 3. Sistema de gestión central y unificada de seguridad Microsoft.[8]

Los componentes que incluye el sistema de gestión central y unificada de seguridad Microsoft (Microsoft Suite de Seguridad) fue desarrollada a partir de varios componentes los cuales operan juntos para proteger la infraestructura de red brindando una protección segura a todos los computadores de la organización. Aunque los componentes de la suite de Microsoft son fácilmente integrables también pueden trabajar con soluciones de terceros

[8] Texto tomado de: VARSALONE, Jesse. Microsoft Forefront Security Administration Guide. [en línea]. Windows Security org,1/1/2008, [citado 1-08-2009], Formato pdf, Disponible en Internet: http://www.windowsecurity.com/forefrontclientsecurity/forefront_administrationguide.pdf

aprovechando así soluciones que la organización ya esté utilizando ayudando a ahorrar costos hasta que se pueda realizar una completa migración como una decisión a futuro.

La suite de Microsoft se compone de 3 categorías principales: Seguridad para los clientes, Seguridad para los servidores y la seguridad perimetral.

- **La seguridad para los clientes incluye:** Sistemas Operativos con versiones business, enterprice, ultimate para el caso de vista, de XP la versión professional y también versiones 2000 professioal (Se puede instalar Forefront Client Security en sistemas operativos que no se puedan unir a un dominio pero no serían administrados mediante la consola central).
- **La seguridad para servidores incluye:** Servidores Exchange, SharePoint y el servidor donde se instala la consola de administración central.
- **La seguridad perimetral incluye:** El servidor Isa Server el cual es un firewall basado en software de fácil configuración. También permite publicar aplicaciones mediante la configuración de IAG donde se publica un túnel seguro en internet por el puerto 443.

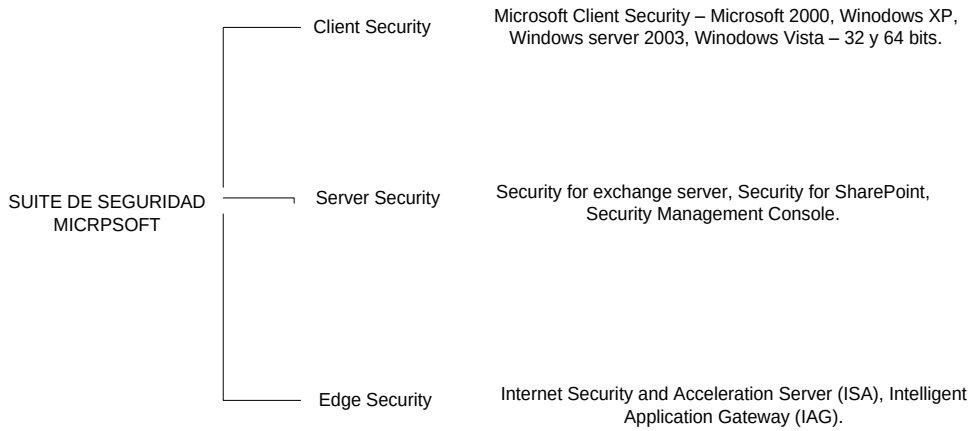


Figura 40: Componentes de la Suite de seguridad Microsoft.

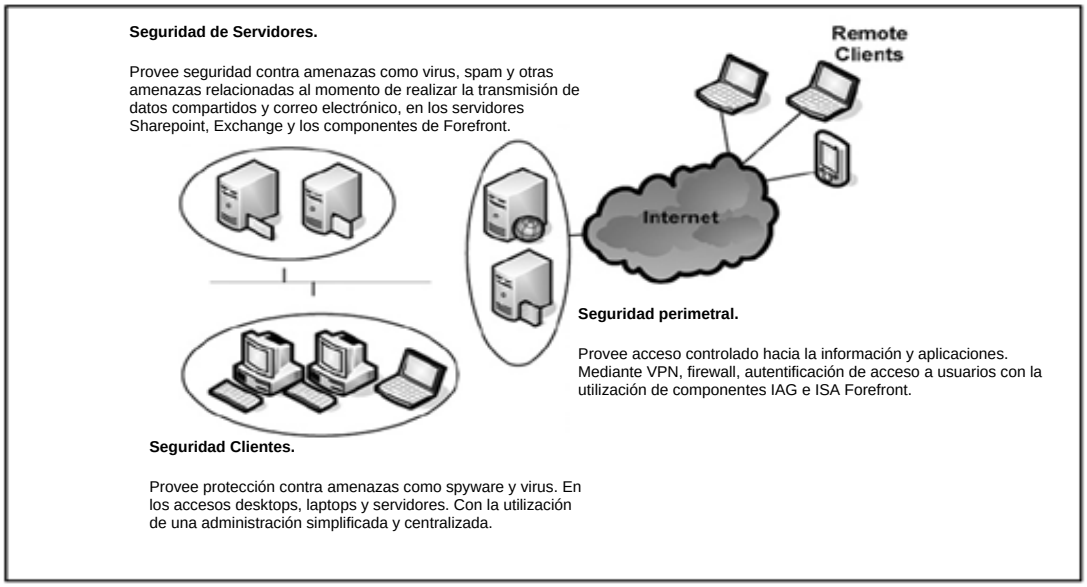


Figura 41: Correlación de los componentes de la suite de seguridad de Microsoft.

3.1 Forefront Client Security (FCS).

Microsoft Forefront Client Security proporciona protección unificada frente al malware para los computadores de escritorio, computadores portátiles y servidores. Con una administración sencilla a través de su consola central de administración mediante una fácil y clara visibilidad de los eventos más importantes de seguridad con acceso a reportes enlazados que llevan rápidamente a los focos de problemas de seguridad desde problemas generales a los más específicos.

FCS es soportando en sistemas operativos desde la versión Windows 2000 profesional hasta Windows 7 en ambientes de 32 y 64 bits. Protegiendo a la red contra el software malicioso como spyware, rootkits, virus, gusanos y troyanos. Entre los componentes que FCS utiliza para realizar su trabajo se encuentran los siguientes servidores:

- **Management Server:** Este es el servidor principal porque maneja la consola central donde todos los clientes antivirus instalados en los computadores de red son monitoreados. Mediante la consola central se puede realizar configuraciones

predeterminadas o modificar las ya definidas en los clientes antivirus. Una gran ventaja de Forefront Client Security es su integración nativa con el directorio activo facilitando a los administradores de red configurar políticas de grupo para el software antivirus e incluso permite utilizar las mismas unidades organizacionales (UO) ya creadas evitando tener que crear nuevos grupos manejados solo por el servidor antivirus.

- **Roles Reporting - Alerting:** Estos roles o bases de datos que se crean en la instalación son importantes porque son los encargados de recopilar y organizar la información de todos los eventos de seguridad de los clientes antivirus.

  El primero recopila toda la información para que puedan ser visualizadas en la consola central mediante informes gráficos y resúmenes ejecutivos fácilmente descriptibles.

  El segundo es el encargado de recopilar toda la información proveniente de los clientes antivirus tomando todos los eventos que de acuerdo a la gravedad de la alerta serán enviados inmediatamente o simplemente ser obviados. Otra habilidad importante del servidor de reporteria (Reporting) es importar los informes ejecutivos en archivos excel, pdf, html para el análisis del administrador de red posteriores.

- **Forefront Client:** El cliente antivirus es el encargado de mantener la seguridad del sistema operativo donde está instalado, el cual ya fue previamente configurado mediante la consola central así realizara su trabajo automáticamente sin la necesidad de que el usuario se preocupe de realizar escaneos en su sistema operativo, permitiéndole enfocarse en su trabajo.

3.1.1 Características de Forefront Client Security.

Forefront Client Security presenta muchas características y beneficios, entre las características principales están la protección antivirus y anti-spyware que trabajan en tiempo real o de forma programada para mantener los computadores de la red protegidos

en contra de las nuevas amenazas que aparecen diariamente. Otra característica importante son los filtros antimalware que son capaces de ejecutarse y analizar los archivos o código malicioso antes de que se ejecuten evitando así que contaminen el sistema.

Existen tres pilares fundamentales en los que se fundamentan las características de Forefront Client Security y estos son los siguientes:

1.- Protección Unificada.

- Motor integrado de antivirus y antispyware.
- Protección en tiempo real con el administrador de filtros de Windows.
- Análisis programados y bajo demanda.
- Herramientas de eliminación malware (scripts de limpieza continuos).
- Análisis de archivos comprimidos y sin compresión.
- Mecanismos de protección avanzada contra malware tecnificado como rootkits y virus polimórficos (Análisis heurísticos).
- Seguridad en sistemas virtualización. FCS puede ser instalado y configurado en máquinas virtuales, como en la tecnología de Microsoft Windows Server 2008 hyper-V.

2.- Administración Centralizada.

- Consola de gestión centralizada que reduce la complejidad de administración reduciendo el tiempo de respuesta.
- Configuración simple de políticas para administrar a los clientes antivirus permitiendo especificar mediante una sola política niveles de seguridad y volumen de alertas generadas en grupos de máquinas.

- Integración con el directorio activo para la implementación ejecución de políticas de grupo basadas en las unidades organizativas (OU) y grupos de seguridad ya implementadas en la organización previamente.
- Integración con WSUS permite instalar actualizaciones de seguridad y los clientes antivirus con una sincronización constante y automática. Evitando su eliminación del cliente antivirus de forma accidental o intencional.
- Actualizaciones de seguridad para los usuarios móviles se pueden realizar en conexión con el servidor central o mediante la conexión directa al sitio de Microsoft Update vía internet manteniendo el sistema actualizado y seguro siempre.

3.- Control y visibilidad de eventos críticos.

- Evaluación de estado de seguridad (SSA). Recolecta información de los registros, metadatos y más archivos del sistema operativo para ayudarle a definir el estado de seguridad del sistema operativo como sus vulnerabilidades de seguridad (Carencia de Service Pack o parches) y otros riesgos basados en las mejores prácticas de seguridad (Debilidad en la clave, cuentas duplicadas, etc.). Como resultado el administrador puede obtener información sumariada y clara de los posibles focos de inseguridad en su red sin la necesidad de analizar información de diversas fuentes por su propia mano.
- Reportes de seguridad vinculados, los cuales permiten adentrarse desde un problema de seguridad general hasta un problema o computador en específico obteniendo información detallada cada vez.
- Entrega de alertas personalizadas sobre los incidentes de seguridad más sensibles entregables por medio de alertas al correo electrónico, permitiendo tomar acciones inmediatas en problemas de seguridad serios.

3.1.2 Configuración e instalación de FCS.

Previamente antes de realizar cualquier instalación exitosa de cualquier software debemos tomar en cuenta los requisitos de hardware y software necesarios para que el mismo funcione bien. FCS no es solo un software antivirus que se instala en cada cliente y simplemente funciona sino que es solo una parte de un sistema central de seguridad el cual es administrado mediante un servidor central pero este servidor central donde se encuentra la consola central de administración y los otros servidores cumpliendo diferentes roles.

FCS tiene cuatro roles los cuales pueden residir en su propio servidor físico dependiendo de los requerimientos a configurar, estos roles son: Management Server, Collection Server, Reporting Server y el Distribution Server.

Durante la instalación de FCS se despliega otro servidor más el Microsoft Operation Manager (MOM) el cual se encarga de recopilar y centralizar los eventos de los clientes antivirus.

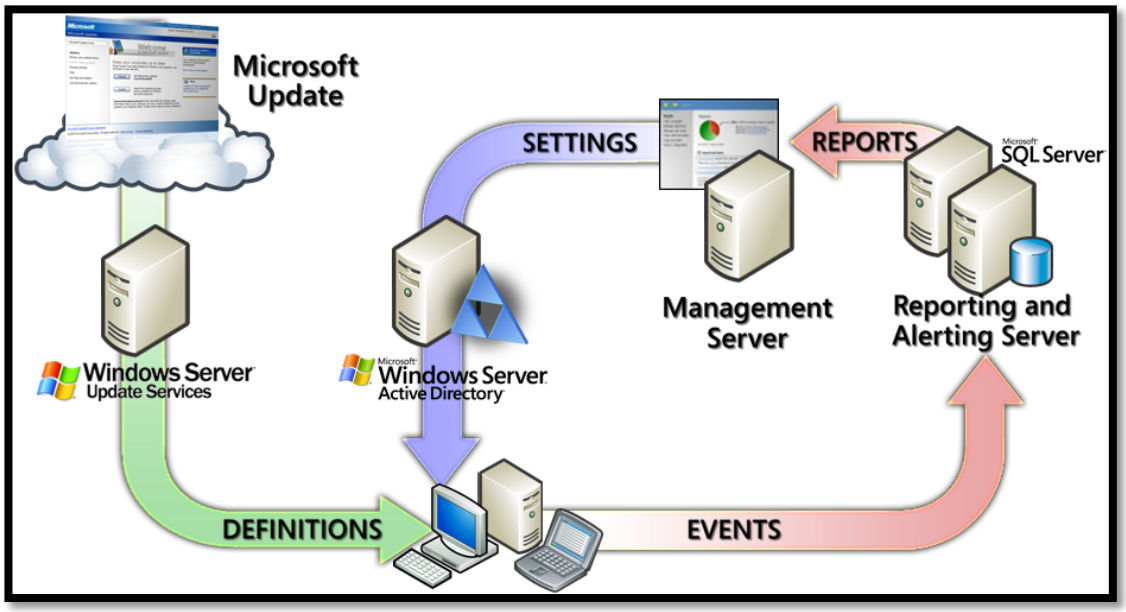


Figura 42: Computadoras de escritorio, computadoras móviles y sistemas operativos de servidor corriendo Microsoft Forefront Client Security,

3.1.3 Topologías de Instalación.

FCS puede ser implementado en numerosas topologías que van desde un único servidor central hasta expandirse a 6 servidores dependiendo del ambiente y los requisitos a satisfacer. Pero las topologías más comúnmente utilizadas son las utilizadas en empresas pequeñas y medianas donde se pueden configurar ambientes de 1 a 3 servidores.

La topología de 3 servidores puede soportar hasta 5000 clientes antivirus. Para empresas grandes se debe utilizar las topologías de 4 a 6 servidores las cuales pueden soportar hasta 10000 clientes antivirus.

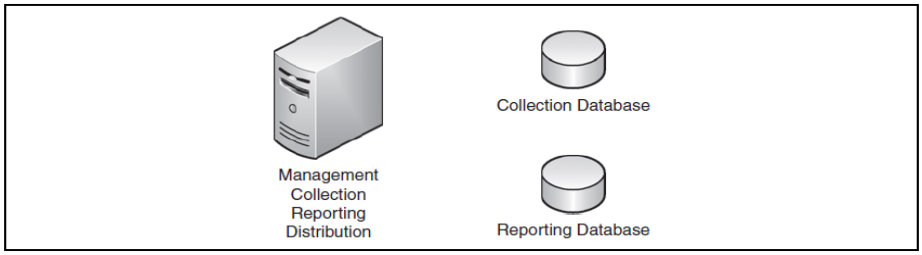


Figura 43: Representa la topología de un solo servidor físico y los roles de las bases de datos.

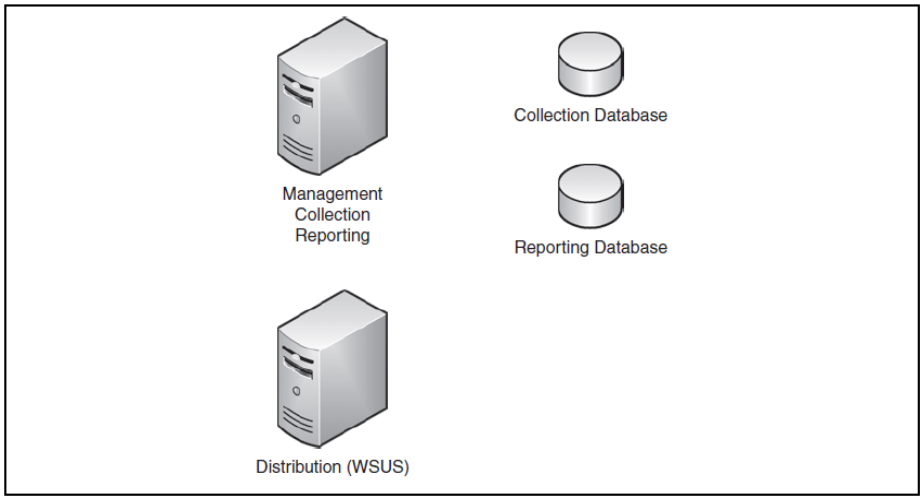


Figura 44: Representa la topología de dos servidores físicos configuración necesaria si la red ya disponía de un servidor WSUS.

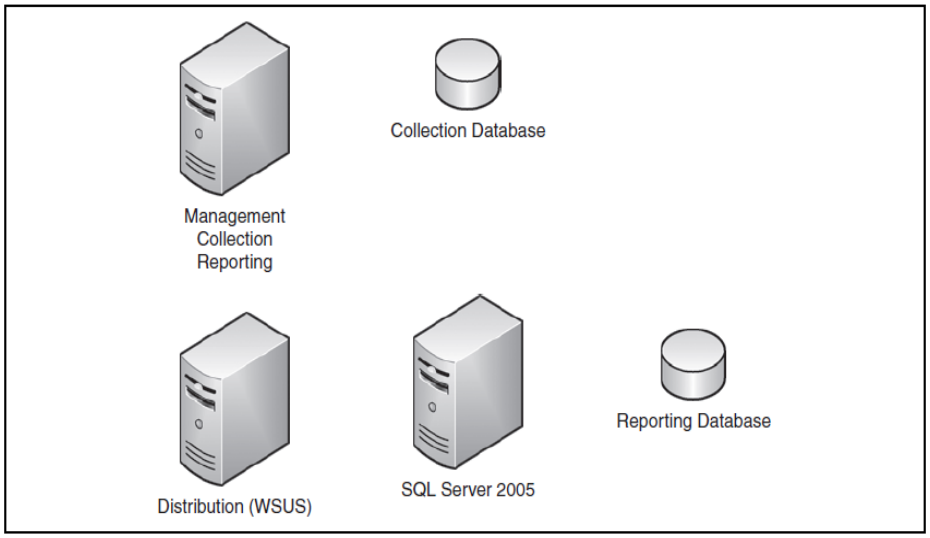


Figura 45: Representación de la topología de 3 servidores, esta topología es necesaria cuando el tráfico de la base de datos de reporteria es muy pesado y afecta el performance de la consola central de FCS.

3.1.4 Descripción de los roles de FCS.

FCS para realizar su protección centralizada y unificada utiliza varios roles los cuales cumplen diversas tareas las cuales se indican a continuación:

Management Server

Este rol es el encargado de manejar el software de Forefront Client Security e incluye la consola central de FCS y el servidor MOM. La consola central presenta un dashboard (Tablero de información centralizado) el cual incluye información referente a malware detectado, vulnerabilidades de seguridad, políticas sin actualizar y alertas de seguridad en general. La consola permite al administrador crear políticas como escaneas contra el malware programado, estado de seguridad de los sistemas operativos, entre las principales.

Collection Server

El rol utiliza como base Microsoft SQL Server 2005 versión Standard o Enterprice dependiendo del número de clientes antivirus que se haya planeado soportar. La base

creada para el Collection Server puede ser configurada en una sola base de datos o puede ser configurada en una base de datos SQL que ya exista en la organización.

Reporting Server

Este rol también requiere el uso de Microsoft SQL Server 2005. Pero como reside en la misma base de datos donde se configura la base de datos Collection Server es necesaria solo una copia de la base de datos SQL Server 2005. La principal aplicación que pertenece a la base de datos SQL es su servicio de Reporting Service, el cual permite a los administradores ver los reportes ya predeterminados en la consola de FCS. La información presentada mediante el rol de Reporting puede ser exportada en archivos los cuales ya no son almacenados en el rol del Collection Server.

Distribution Server

El rol asignado al Distribución Server pertenece al repositorio centralizado de actualizaciones WSUS el cual se encarga de entregar las firmas antimalware y actualizaciones de seguridad de los sistemas operativos en la red de la organización.

3.1.5 Requisitos para la instalación del servidor FCS.

Una vez que se han aclarado cómo funcionan los roles que se generan al instalar el servidor de FCS, requerimientos de software, hardware, topologías de instalación así como los sistemas operativos donde se puede instalar los clientes antivirus. Se puede proceder a la instalación de la consola de FCS.

Debido a que la cantidad de computadores en la mayor parte de las organizaciones es reducido en relación de países más del primer mundo, se tomara como ejemplo la instalación de la topología de un servidor. Los requisitos necesarios en el servidor base son tener instalado:

- Windows Server 2003 Standard o Enterprice R2 con SP2. (Incluye MMC 3.0 requisito).
- SQL Server 2005 Standard con SP2 con su servicio de Reporting Services.
- .Net Framework 2.0.
- Internet Information Services 6.0.
- ASP.NET
- FrontPage Server Extensions.
- Group Police Manager Console GPMC SP1
- Windows Server Update Services WSUS 3.0.

3.1.6 Consola de administración central FCS.

La consola central de administración consta de mucho información visual sumarizada la cual permite al administrador de red conocer el estado de seguridad de su red en forma general de un solo vistazo sin la necesidad de investigar varias fuentes para determinar la fuente de un ataque de software malicioso u otros problemas relacionados.

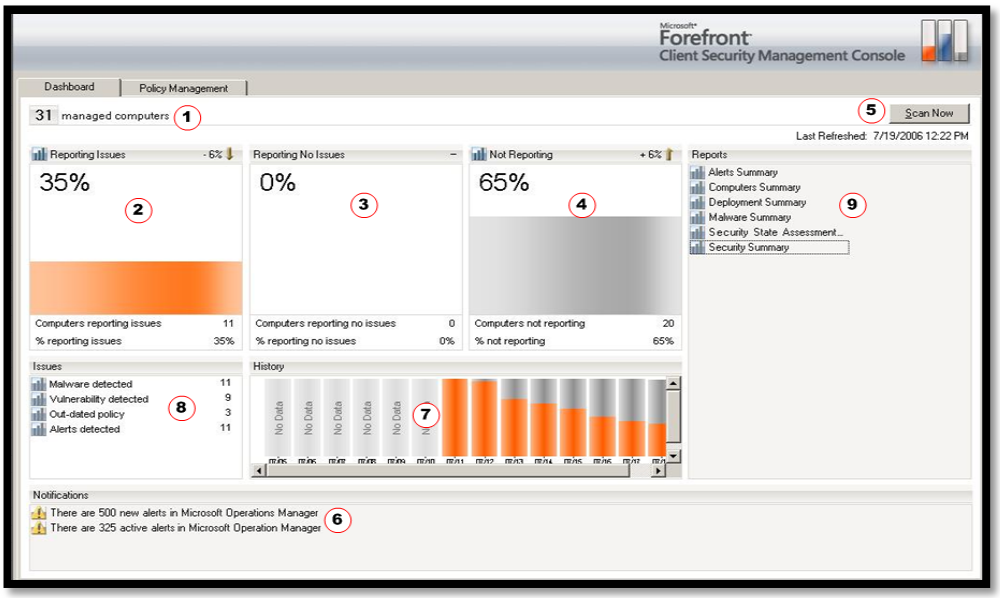


Figura 46: Consola central de administración FCS.

A continuación se detalla las funciones de la consola central indicada mediante los números indicados en la gráfica anterior:

1. Numero de computadoras manejadas por la consola, el número solo toma en cuenta los computadores que tienen instalado en cliente antivirus.
2. Porcentaje de computadores que han reportado problemas las últimas 24 horas.
3. Porcentaje de computadores que no han reportado problemas las últimas 24 horas.
4. Porcentaje de computadores que no se han reportado al servidor central las últimas 24 horas. Este porcentaje suele ser indicativo de problemas de conexión o de cantidad de computadores móviles.
5. Mediante esta opción se puede realizar escaneos por demanda rápidos o completos de ser necesario a cualquier computador agregado a la consola. Se basa en la integración con el directorio activo.
6. Indica el número de alertas que se han generado en el servidor MOM el cual permite visualizar en la consola del servidor MOM los eventos generados por cada computador con sus horas y con un detallado informe de los problemas que se han generado en la estación.
7. Es un gráfica historial de 14 días pasado, mediante la misma podemos visualizar el desempeño de la consola o los problemas de causados de seguridad causados anteriormente para tener una visión global de seguridad de la red en el tiempo.
8. Este menú es de gran importancia porque no proporciona vínculos a los problemas que no han sido solucionados como malware detectado, vulnerabilidades de seguridad, policías de grupo no desplegadas y alertas de seguridad en general que no han sido tomadas en cuenta.
9. Es otro de los menús importantes debido a que nos da acceso a los reportes que se han generado por parte del servidor de Reporting.

3.1.7 Reportes de seguridad de la consola FCS.

Los reportes proporcionados por el servidor de Reporting son una herramienta importante para el administrador de red porque le permiten determinar el origen de los problemas de malware, determinar si existen epidemias propagándose por la red,problemas del estado de seguridad de los sistemas operativos como falencia de service packs o parches, etc.

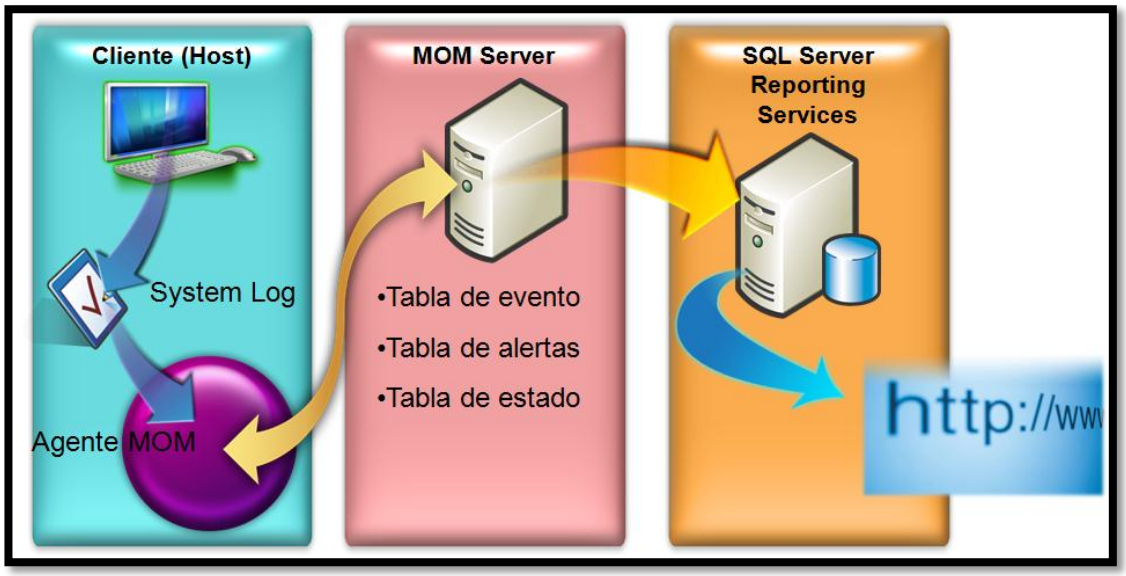


Figura 47: Captura, almacenamiento y generación de los reportes de seguridad FCS.

Existen 6 reportes de seguridad generados por el rol de Reporting los cuales se detallaran a continuación:

Resumen de alertas: es un informe sumarizado de toda la información recopilada por los agentes instalados en todos los computadores de la red. Muestra un pequeño resumen de los informes presentes en la consola central e información a parte las principales alertas (Top 10), el número de computadores con problemas de seguridad (Virus, Vulnerabilidades, Alertas, Políticas nos actualizadas), principales virus detectados, historiales con información de alertas de seguridad y vulnerabilidades descubiertas.

En fin es un resumen que a pesar de la cantidad de información que presenta es de fácil entendimiento una vez que se conoce cada gráfica y vinculo presentado.

Figura 48: Menú de acceso a los reportes de seguridad de la consola FCS.

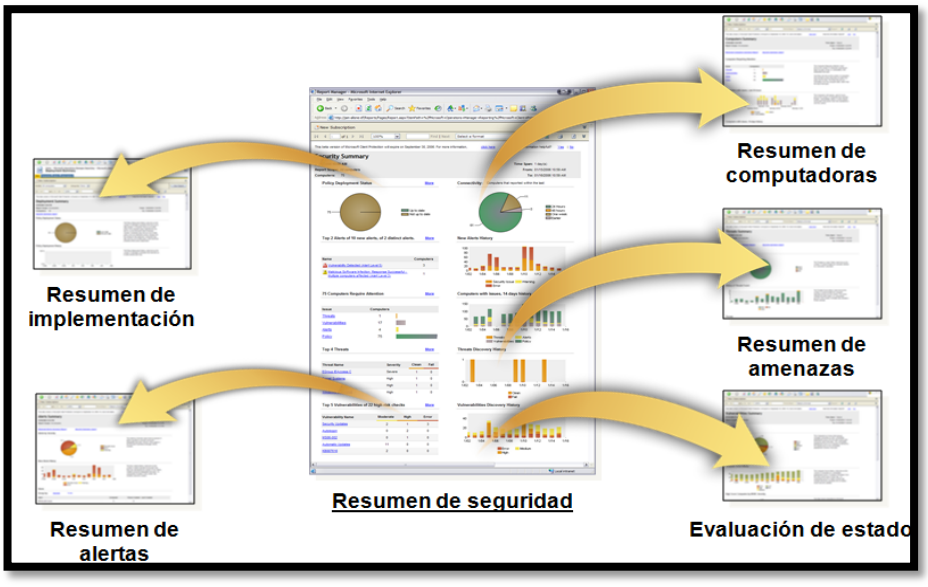


Figura 49: Reporte de Resumen de alertas. Presentado por el rol de Reporting de FCS.

Resumen de equipos: Este reporte informe presentan información acerca de los equipos administrados por la consola de FCS.

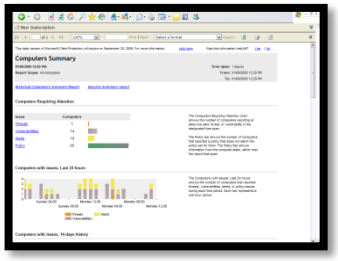


Figura 50: Informe Reporte de equipos administrados consola FCS.

Resumen de implementación: Este reporte presenta información sobre el estado de las actualizaciones descargadas por la consola y como están siendo diseminadas en la red. Con indicadores gráficos con porcentajes y problemas de implementación.

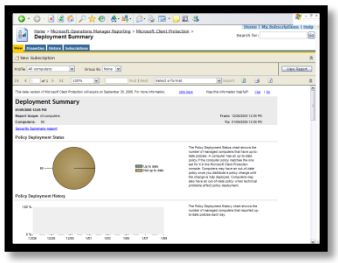


Figura 51: Informe Reporte de Implementación consola FCS.

Resumen de la evaluación de estado de seguridad (SSA): Este reporte es uno de los más importantes porque proporciona información sobre cuáles son las actualizaciones necesarias para cada equipo.

Y otra información indispensable para conocer el estado de la seguridad de los clientes en la red.

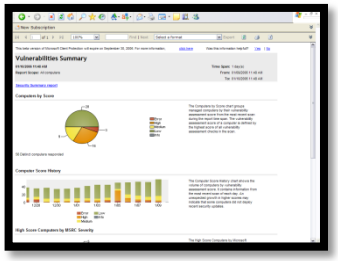


Figura 52: Informe Resumen de la evaluación de estado de seguridad consola FCS.

Resumen de malware: Este informe presenta una información su marizada de todos los ataques que los equipos han sufrido en periodos de tiempo, permitiendo conocer cuáles son los epidemias desatadas en la red así como cual computador fue el responsable y dando acceso a links de ayuda para solventar estos problemas de forma eficaz. Así si se necesita una cierta actualización la misma puede ser debidamente descargada e implantada en la red.

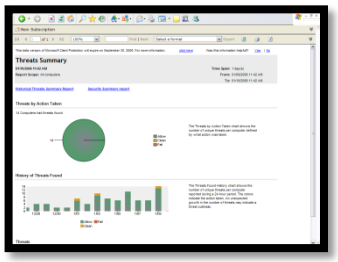


Figura 53: Informe Resumen de malware consola FCS.

Resumen de seguridad: Este informe presenta información de los principales problemas de seguridad relacionados con todos los problemas ocasionados en la red.

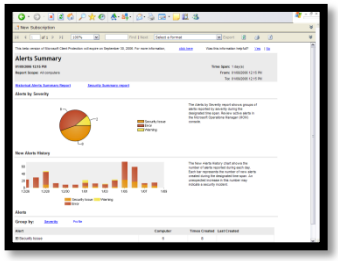


Figura 54: Informe Resumen de seguridad consola FCS.

3.1.8 Configuración y despliegue de políticas FCS.

En la consola de FCS se encuentra un vínculo al menú de administración de directivas donde se configuran las políticas que afectaran a los clientes antivirus. Para realizar estas configuraciones existen las siguientes pestañas:

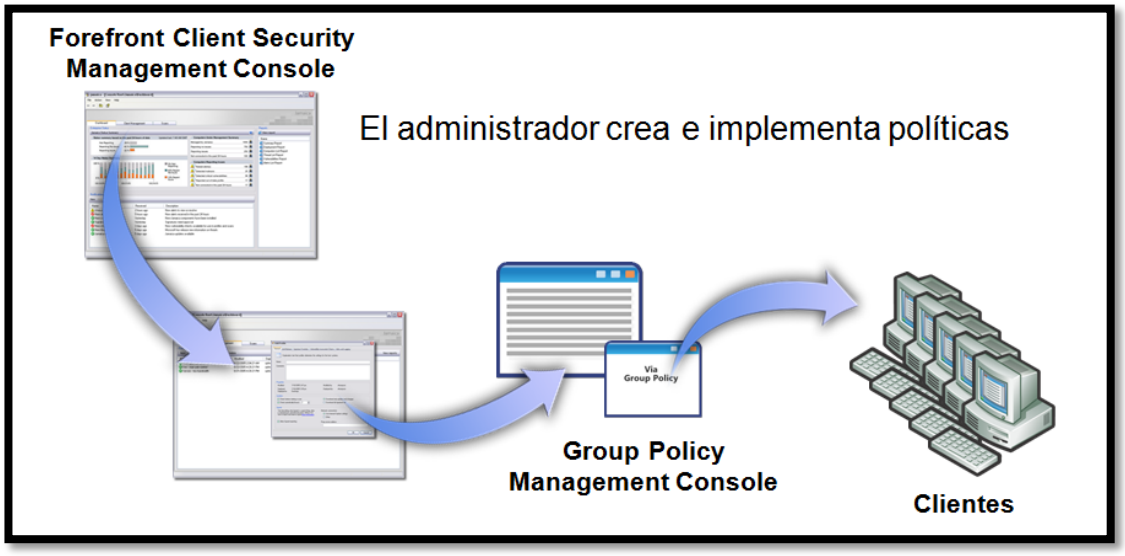


Figura 55: Despliegue políticas de seguridad desde la consola de FCS.

General: Es donde se determina el nombre de la política y se deja una descripción de la misma.

Protección: En esta pestaña podemos habilitar o deshabilitar la protección antivirus y de la spyware. Es escáner en tiempo real, así como la hora que los mismos iniciaran. También se puede configurar el escáner SSA que toma información de las computadoras para determinar sus falencias de seguridad.

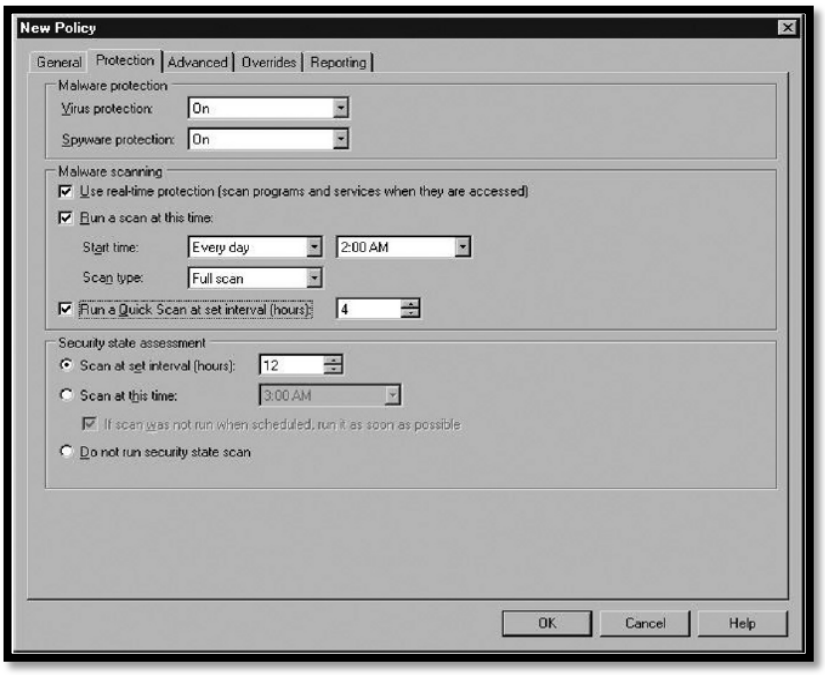


Figura 56: Pestaña "Protection" configuración políticas de seguridad consola FCS.

Avanzadas: En esta pestaña se configura cuando se realizaran las actualizaciones y si los computadores pueden conectarse a al sitio de Windows Update cuando el servidor WSUS no esté disponible. También permite configurar la forma de actuar cuando se realizan los escaneos antivirus como: Excluir archivos de ciertas locaciones del sistema operativo u omitir ciertas extensiones. Utilizar el escáner heurístico o después de cuánto tiempo eliminar los archivos en cuarentena. Algo importante de esta pestaña es que permite determinar al acceso o no la consola del cliente antivirus o solo permitir el uso de configuraciones básicas por ejemplo: Configurar el antivirus para que realice un escáner a las 11 am y el usuario de la estación no podrá detenerlo porque no tiene los permisos para acceder a la consola o se

puede eliminar directamente archivos infectados sin dejar la intervención del usuario que abrió dicho archivo.

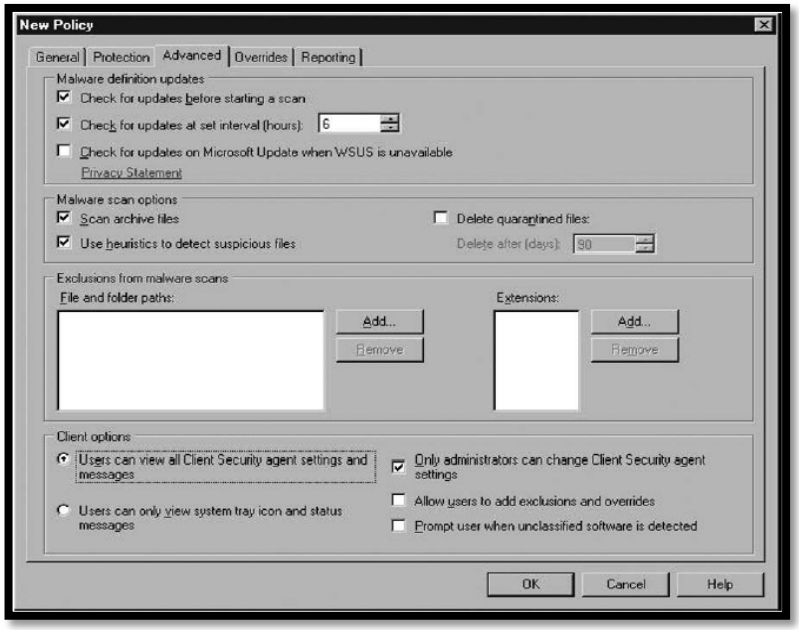


Figura 57: Pestaña “Advanced” configuración políticas de seguridad consola FCS.

Reportes: La última pestaña permite configurar el nivel de seguridad de la política, es decir cuántas alertas se enviaran a la consola central. Para mejor comprensión se plantea el siguiente ejemplo: Si es una política para servidores es de vital importancia que las alertas de seguridad sean enviadas lo más rápido posible a la consola central para que el administrador pueda tomar acciones correctivas sobre la marcha y evitar que los servidores colapsen por el ataque de algún software malicioso entonces la alerta deberá ser configurada en nivel 5.

Pero si la política va a ser desplegada en computadores de poca relevancia como los de recepción o de personal que casi no pasa en la organización un nivel 2 o el más bajo debe

ser configurado, esto para evitar que la consola central sea bombardeada con demasiada información de computadores menos importantes.

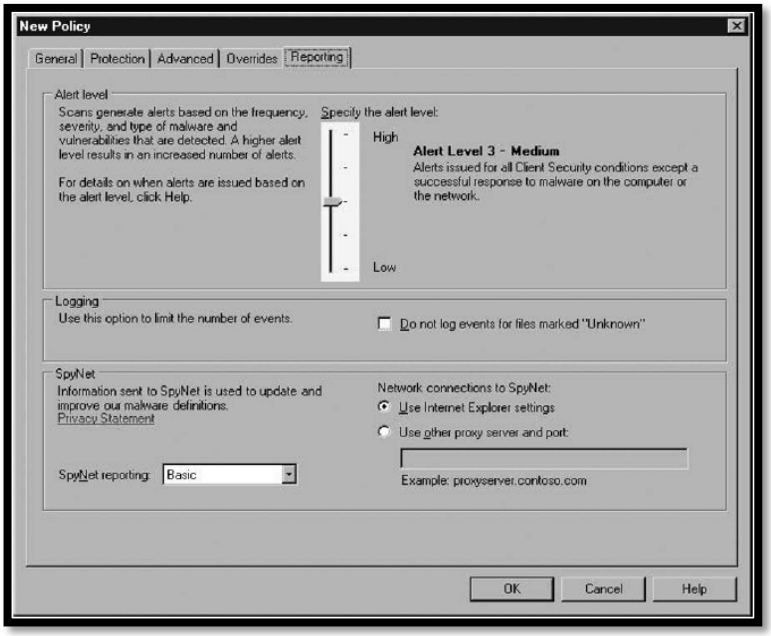


Figura 58: Pestaña “Reporting” configuración políticas de seguridad consola FCS.

Despliegue: Una vez terminada la configuración de a política se puede proceder al despliegue de la misma, es cuando se aprovecha la integración del servidor FCS al directorio activo de la organización porque la política puede ser desplegada en las unidades organizaciones, grupos de seguridad o importar la política a un archivo para poder desplegarla en computadores que no les es posible comunicarse con el servidor central pero que es necesario mantenerlos controlados. Una vez desplegada la política será actualizada en una hora aproximadamente en los clientes o si se reinicia el equipo se actualizara una vez iniciado el equipo, también se puede forzar la política mediante línea de comandos con el comando **gpupdate/force.**

También se debe tener en consideración que las políticas pueden ser desplegadas en una por vez en cada unidad organizacional, es decir si se aplica una nueva política

automáticamente la anterior policita es totalmente des configurada y se toman los valores de la nueva política.

Figura 59: Menú de configuración para despliegue de políticas de seguridad consola FCS.

Figura 60: Menú de configuración para despliegue políticas en UO de seguridad consola FCS.

3.1.9 Instalación del Cliente Antivirus.

El agente de Forefront Client Security puede ser instalado en versiones de Windows 2000 SP4, Windows XP SP2, Windows Server 2003 (R2/SP1), Windows Vista y Windows 7. Antes empezar con la instalación del agente es preferente que se realice en sistemas operativos con las últimas actualizaciones de seguridad y eliminar cualquier software antivirus que haya sido instalado previamente. En el caso de Windows Vista se debe deshabilitar Windows Defender. Para evitar una inflación manual de los clientes se puede crear un Logon script con la ruta y las especificaciones para su instalación vía servidor.

Para realizar la instalación manual se debe copiar la carpeta donde se encuentra instalador del agente y luego ejecutar vía línea de comandos los siguientes parámetros:

/CG <ManagementGroupName>	Specify the MOM management group name. Default is ForefrontClientSecurity.
/MS <ManagementServerName>	The fully qualiÞed domain name of the Management server. Ex: srv1.test.com.
/I	Specify a folder to install the client in besides the default.
/NOMOM	Tell **ClientSetup.exe** not to install the MOM agent. Used on a separate Collection Server.

Figura 61: Información necesaria ejecutar la instalación del agente FCS.

Ejemplo: Código archivo de instalación .bat El cual fue generado para ser realizar la instalación desatendida es decir ejecutando el archivo .bat como un archivo un instalador .exe, sin necesidad de ejecutar el código en línea de comandos.

- **Clientsetup.exe:** Instador cliente Microsoft Forefront client security.
- **MS AD3:** Nombre del servidor donde se encuentra el software servidor FCS.
- **CG ForefrontClientSecurity:** Especifica el grupo de seguridad utilizado por FCS para realizar sus respectivas configuraciones.
- **/L c:\forefront\:** Crea y mapea la carpeta donde se instalara el software cliente en la maquina cliente. (Almacenando información del FCS cliente, log de seguridad, etc)

Ejemplo: Script creado para el despliegue del agente FCS en el LTIC.

```
D: \\client
clientsetup.exe /MS AD3 /CG ForefrontClientSecurity /L
c:\forefront\
```

El cual se guarda en un archivo .bat que puede ser ejecutado como un archivo .exe.

Una vez ejecutado el Logon script o ejecutado la línea de comandos el agente es instalado en la estación de trabajo y está lista para ser monitoreada por el servidor de FCS.

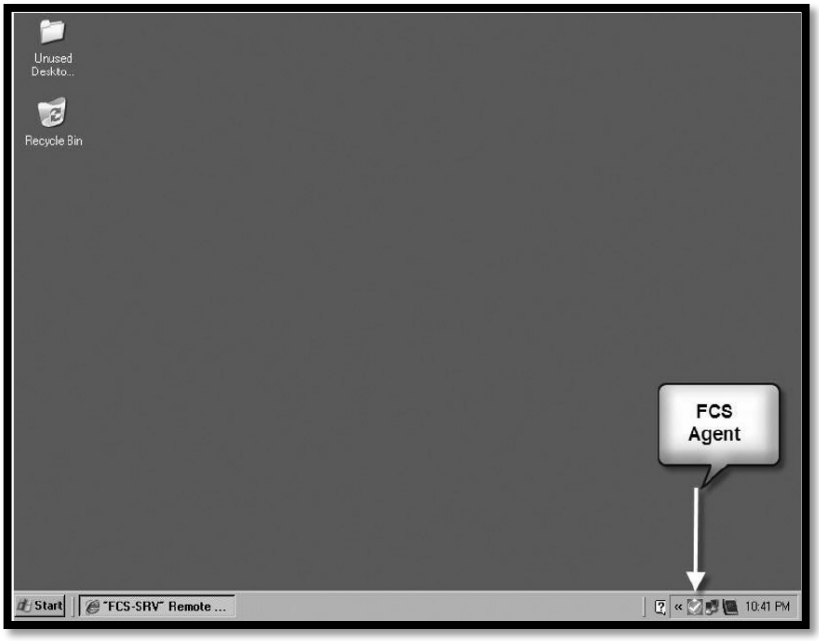


Figura 62: Estado de agente una vez realizada una instalación exitosa agente FCS.

Después de desplegado el agente empezara a enviar información al servidor sobre el estado de actualización del cliente antivirus y el estado de seguridad del sistema operativo donde se está ejecutando. El agente protege el sistema contra el software maligno, dependiendo de la configuración asignada a la estación de trabajo por medio de su unidad organizacional el agente trabajara de la forma asignada actuando automáticamente contra el software maligno o dejando decidir al usuario de la estación de trabajo.

Figura 63: Tecnología Smart Clean detectando un archivo infectado con el virus de prueba EICAR. Smart Clean permite seleccionar una acción.

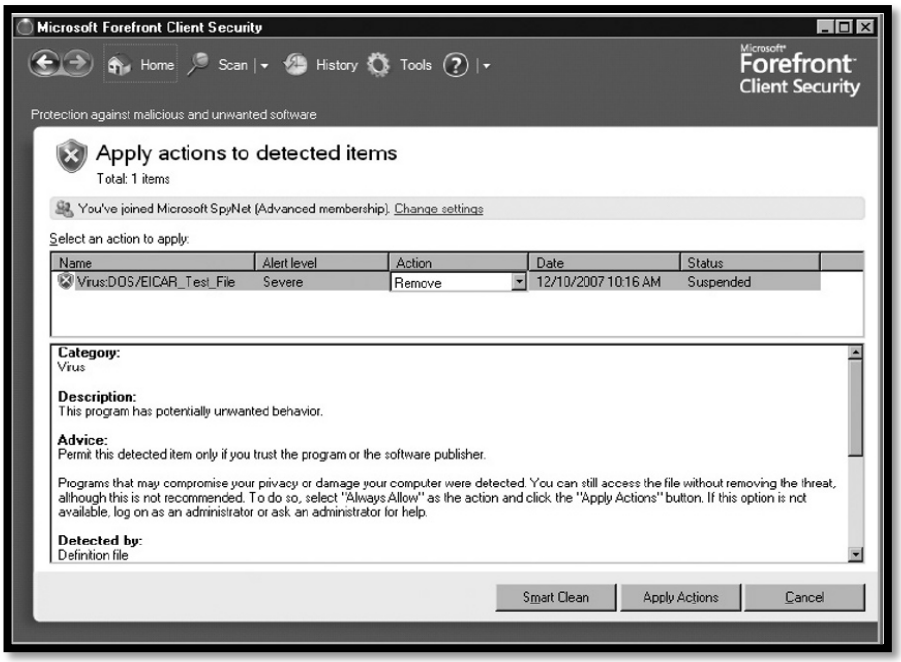


Figura 64: Ventana FSC donde el usuario decide que acción tomar bajo un ataque de software maligno mediante la información entregada.

3.2 Windows Server Update Services (WSUS).

El software Microsoft WSUS provee una herramienta fácil de instalar y administrar. Permitiendo manejar las actualizaciones de seguridad y actualizaciones del software Microsoft presente en la red de la organización. Aunque WSUS no es el único software capaz de realizar esta tarea pero una gran ventaja sobre aplicaciones de terceros es que se trata de una aplicación gratuita lo cual indica la preocupación por parte de Microsoft para que el software Microsoft que utilizan las organizaciones permanezca siempre actualizado.

Antes de instalar el servidor WSUS se debe tener dos cosas presentes, que topología usar y los requerimientos necesarios. La instalación y configuración de políticas de grupo se enfocara en la versión WSUS 3.0 así como la importancia del puerto 8530.

3.2.1 Topologías de instalación.

Existen diversas topologías que pueden ser seleccionadas dependiendo de las necesidades del ambiente de red en la organización. La topología de un solo servidor es la más simple la cual funciona de una forma muy sencilla. Primero descarga las actualizaciones del sitio de Microsoft Update para luego distribuirlas entre los servidores, pc de escritorio y laptops mediante el uso de la red interna de la organización.

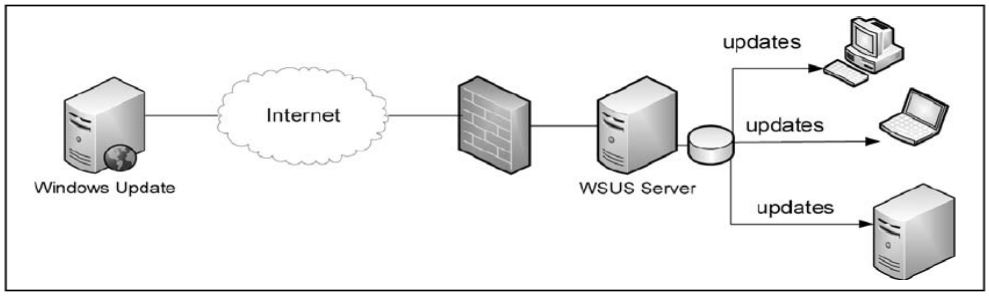


Figura 65: Topología de un solo servidor de WSUS.

Una vez instalado el servidor debe sincronizarse con el sitio de Microsoft Update para mantener las actualizaciones al día. La primera vez que se sincronice el servidor puede tomar varias horas dependiendo de la conexión de internet y el número de actualizaciones que debe descargar. Para evitar recargar el trabajo de un solo servidor o si existen distintas locaciones geográficas de la empresa es necesario configurar “Server hierarchies”. Donde un servidor que hace de rol principal descarga las actualizaciones de sitio de Microsoft Update y los demás servidores se alimentan de este servidor principal una vez sincronizados ellos son los encargados de repartir las actualizaciones por la red interna.

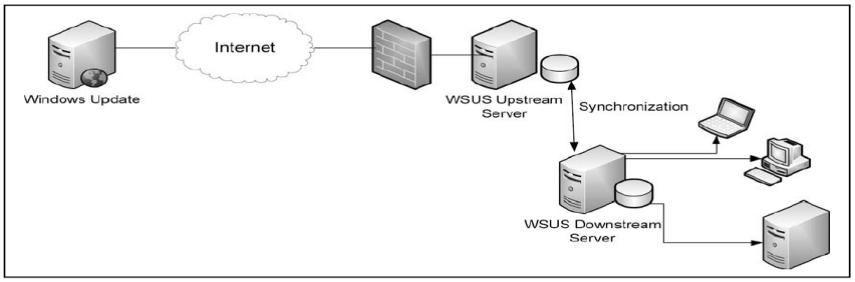


Figura 66: Topología WSUS Server hierarchies.

3.2.2 Requisitos y configuración WSUS.

Una vez seleccionada la topología se debe verificar si la misma cumple con los requisitos disponibles en la organización. Aunque WSUS puede ser instalado en Windows Server 2008, la siguiente tabla hace referencia a los requisitos en Windows Server 2003.

Server Operating System	System Requirements
Windows Server 2003 Service Pack 1 or higher	Internet Information Services (IIS) 6.0 Any updates for Background Intelligent Transfer Services (BITS) 2.0 and WinHTTP 5.1 .NET Framework 2.0 Redistributable Package Report Viewer Redistributable 2005 Microsoft Management Console (MMC) 3.0 SQL Server 2005 Service Pack 1 (optional) 1GB (minimum) of free space on the system partition 2GB (minimum) of free space to store the database files 20GB (minimum) of free space on the volume that will store the content

Figura 67: Requisitos servidor WSUS en Windows Server 2003

Una vez que se ha cumplido con los requisitos mínimos en la plataforma de Windows Server 2003, se procede a instalar la consola. Con el CD de instalación o el ejecutable. Es un proceso sencillo si se trata de una topología de un solo servidor porque todos los valores por defecto se mantienen.

Aunque muchas de las configuraciones de conexión como la utilización de proxy no son de gran problemática al ser inicializados se debe tomar en cuenta las configuraciones de idioma, actualizaciones por producto a descargar y el tipo de actualización a sincronizar.

Porque de estas dependerá el tamaño de disco duro necesario y si en verdad se está sincronizando todos los productos necesarios para mantener nuestra red segura.

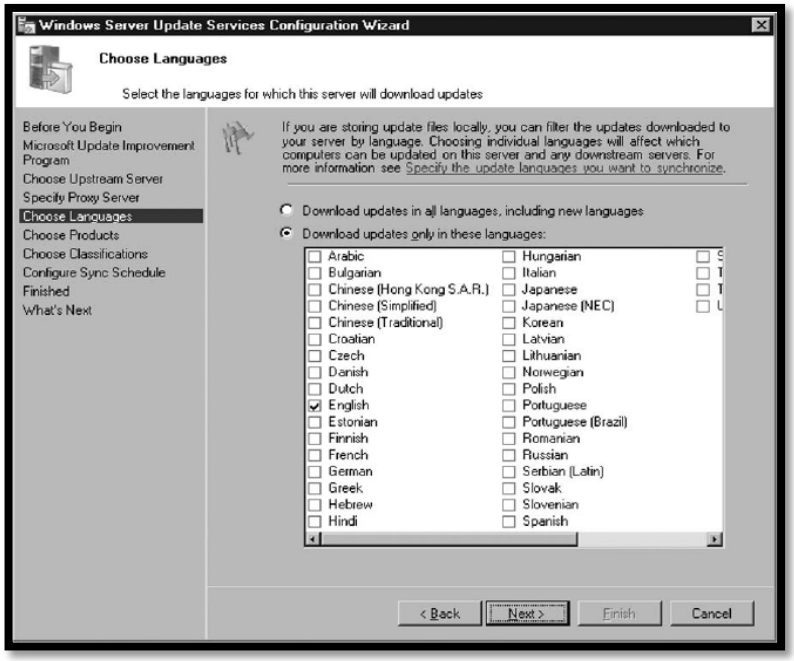


Figura 68: Menú de configuración WSUS, selección del idioma actualizaciones a descargar.

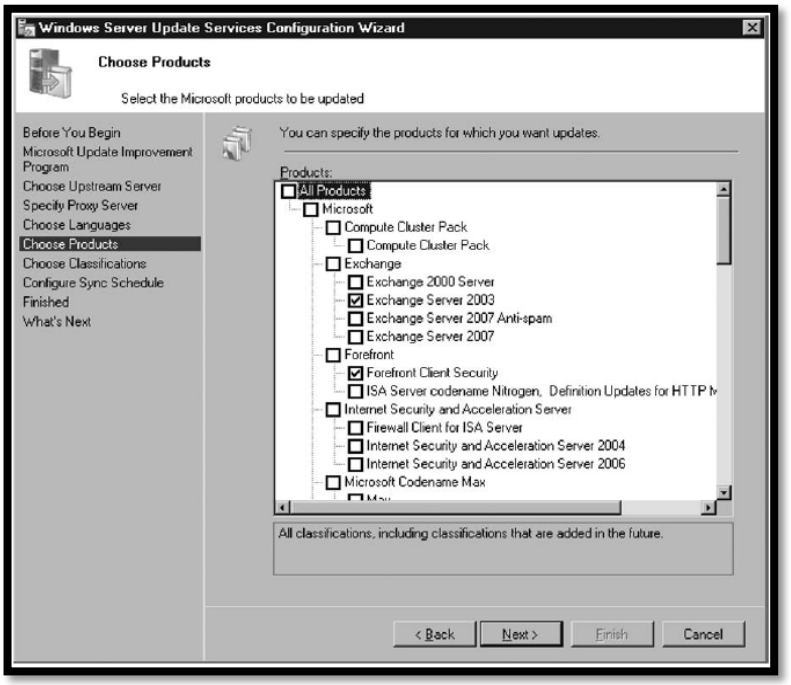


Figura 69: Menú de configuración WSUS selección de productos a descargar.

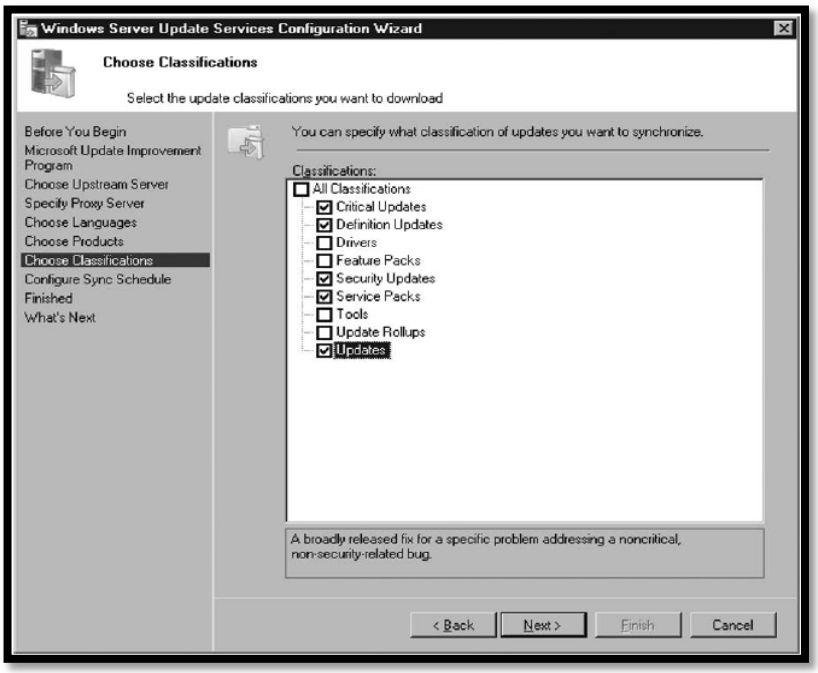


Figura 70: Menú de configuración WSUS selección de los tipos de actualización a descargar.

3.2.3 Políticas de grupo para actualizaciones.

Existe una última configuración que es de vital importancia para que la consola pueda repartir sus actualizaciones de forma centralizada. Con base en el Directorio Activo se configura una política de grupo global para que todo el dominio acuda al servidor WSUS a tomar sus actualizaciones y no mediante el uso de internet.

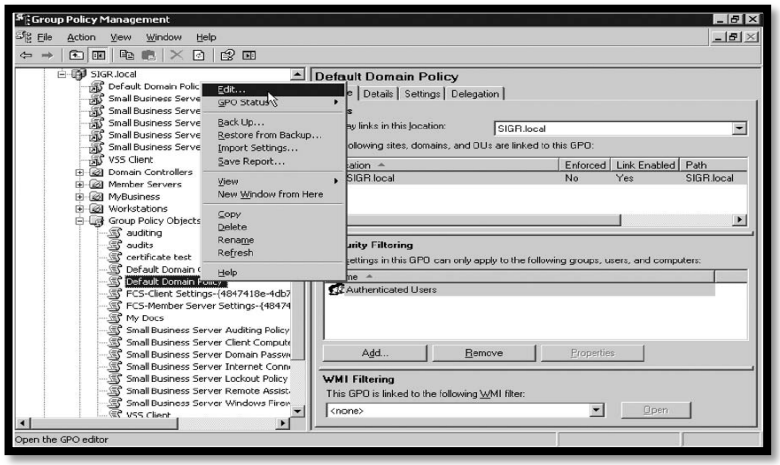


Figura 71: Configuración política de grupo global para apuntar al servidor de actualizaciones WSUS.

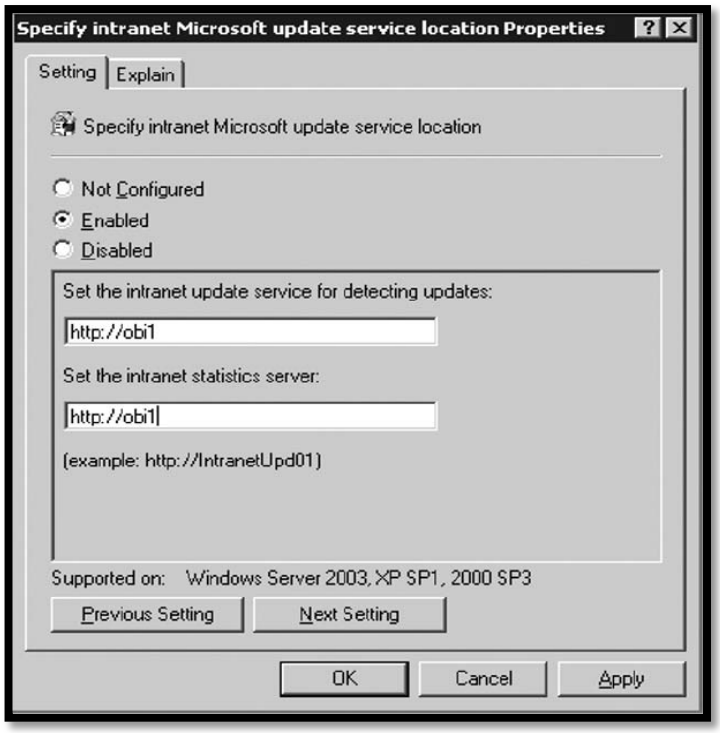


Figura 72: Política de grupo direccionando al servidor WSUS inicializando el nombre del servidor o dirección de red.

3.2.4 Consola WSUS.

En la misma forma con la consola de FCS se encarga de ver el estado de seguridad de las computadoras en la red. La consola de WSUS se encarga de sincronizarse con el sitio de Microsoft Update y ver el estado de las actualizaciones de seguridad de las computadoras en la red. Las dos consolas se complementan todo el tiempo debido a que las actualizaciones de seguridad son parte importante para mantener los equipos seguros. Por ejemplo: En el caso del conocido virus Conficker, ataca a equipos con una vulnerabilidad especifica es decir si los equipos no poseen esta actualización por más que el cliente antivirus tenga la firma antimalware no podrá eliminar el virus porque siempre volverá a atacar el equipo hasta que la vulnerabilidad sea corregida.

La interface de la consola utiliza como base MMC. En menú principal tiene tres componentes principales: Console Tree, Details Pane, Actions Pane. Cada vez que se selecciona una de estas opciones se presenta distinta información la cual es relacionada.

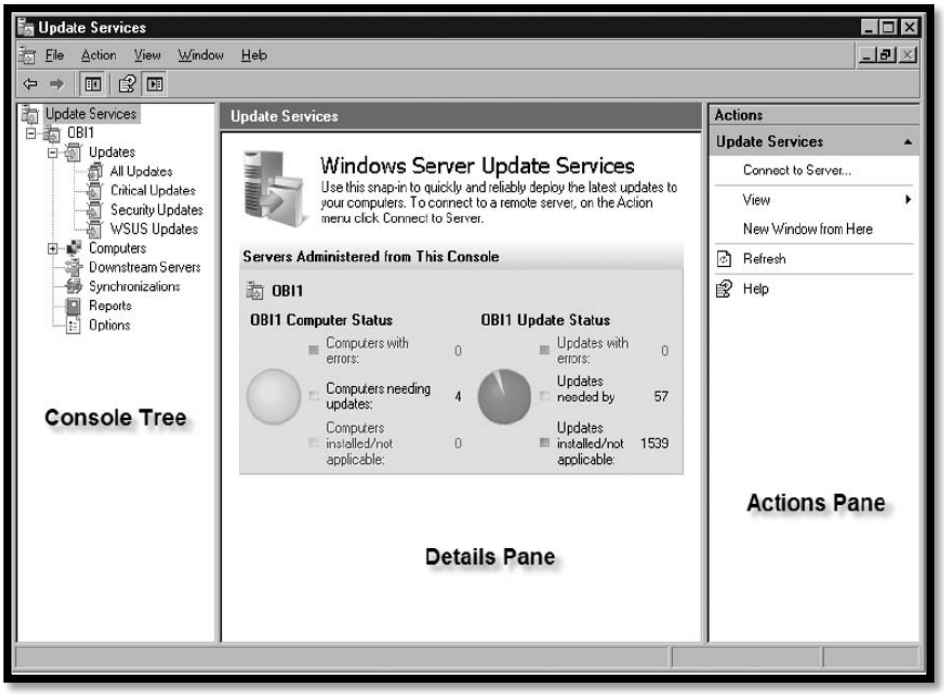


Figura 73: Consola central Windows Server Update Services versión 3.0

3.2.5 Servicios de actualización.

En el menú “Console Tree” se encuentran nodos los cuales presentan todos los servicios que la consola WSUS puede manejar.

Nodo Updates: Es el que recopila los sub nodos encargados de manejar y actualizar todas las actualizaciones descargadas. Las cuales podrán ser aprobadas o desaprobadas para su entrega organizada y automatizada por la red de acuerdo a los grupos creados para este efecto. Es importante mencionar que en la consola aparecerán todas las computadoras presentes en la red mientras que en la consola de FCS solo aparecerán los computadores con los clientes antivirus desplegados, es decir los agentes de FCS. Los sub nodos son los siguientes:

- **All Updates:** Lista todas las actualizaciones descargadas y por medio de un informe visual se puede visualizar el porcentaje de despliegue en las computadoras de la red.
- **Critical Updates:** Existe una gran cantidad de actualizaciones que se descargan al sincronizar el servidor con el sitio Microsoft Update pero existen actualizaciones de seguridad más importantes que otras las cuales deberían ser aprobadas primero antes que otras de menos relevancia. Así que todas las actualizaciones listadas en este sub nodo son de vital importancia que sean desplegadas.
- **Security Updates:** En este sub nodo se listan las actualizaciones de seguridad menos importantes pero que una vez aprobadas todas las actualizaciones críticas se debe planear el despliegue de estas actualizaciones.
- **WSUS Updates:** En este sub nodo solo se listan las actualizaciones de la consola WSUS.

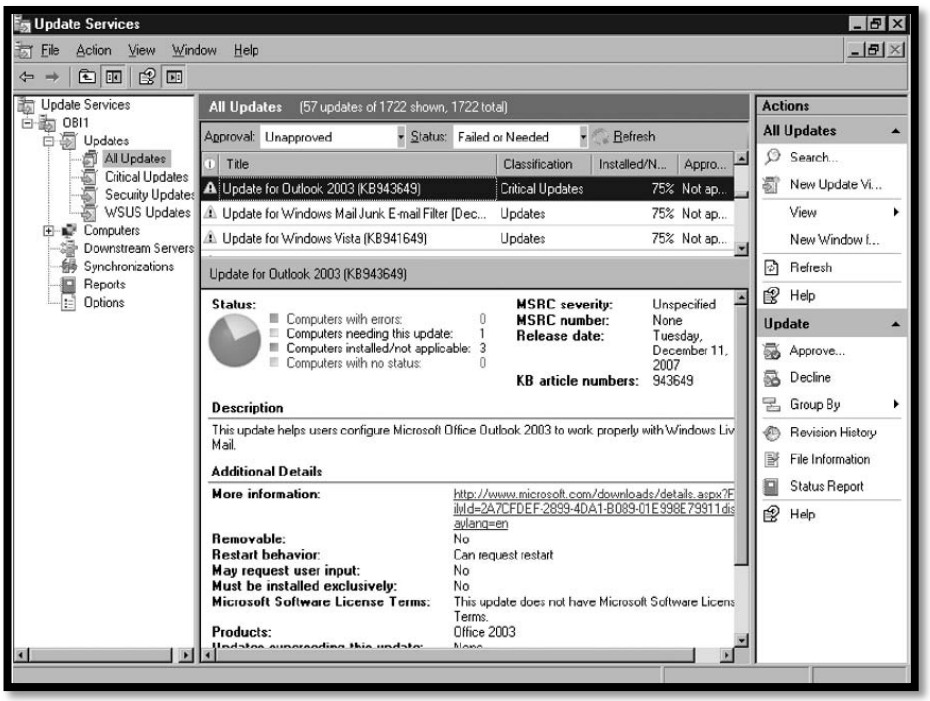


Figura 74: Consola WSUS. Sub nodo All updates. La cual indica el estado de las actualizaciones descargadas.

Aprobación o Declinación de actualizaciones: Una vez descargadas las actualizaciones podemos decidir si desplegarlas o no. Realizar su despliegue en distintas Unidas Organizaciones o hacerlos en todas las computadoras de la red. Pero se debe tener en cuenta que al realizar estos despliegues se debe tomar en cuenta si son del idioma correcto y sin no han sido ya desplegadas.

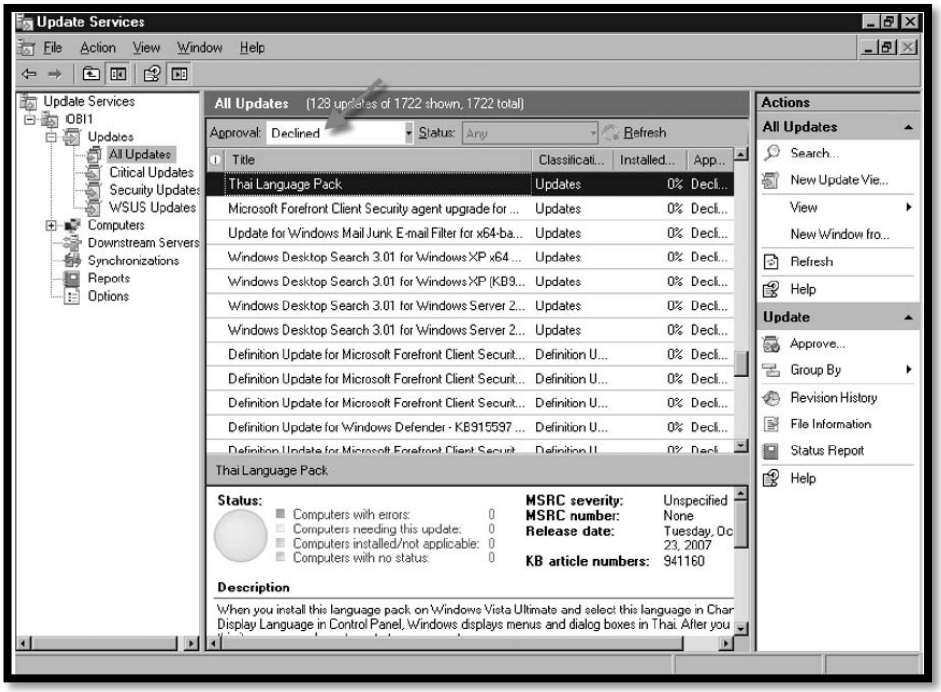


Figura 75: Consola WSUS. Representa la aprobación o la declinación de actualizaciones.

Nodo Computers: Este nodo es donde podemos visualizar todos los computadores de la red. Los cuales pueden ser organizados dependiendo de la forma que desee el administrador de red como ayuda para mantener sus estaciones de trabajo actualizadas.

Una vez que se han reconocido todas las computadoras de la red se agregan a un grupo llamado “Sin asignar”, de donde el administrador puede tomar las computadoras para organizarlas de acuerdo a como quiera desplegar las actualizaciones.

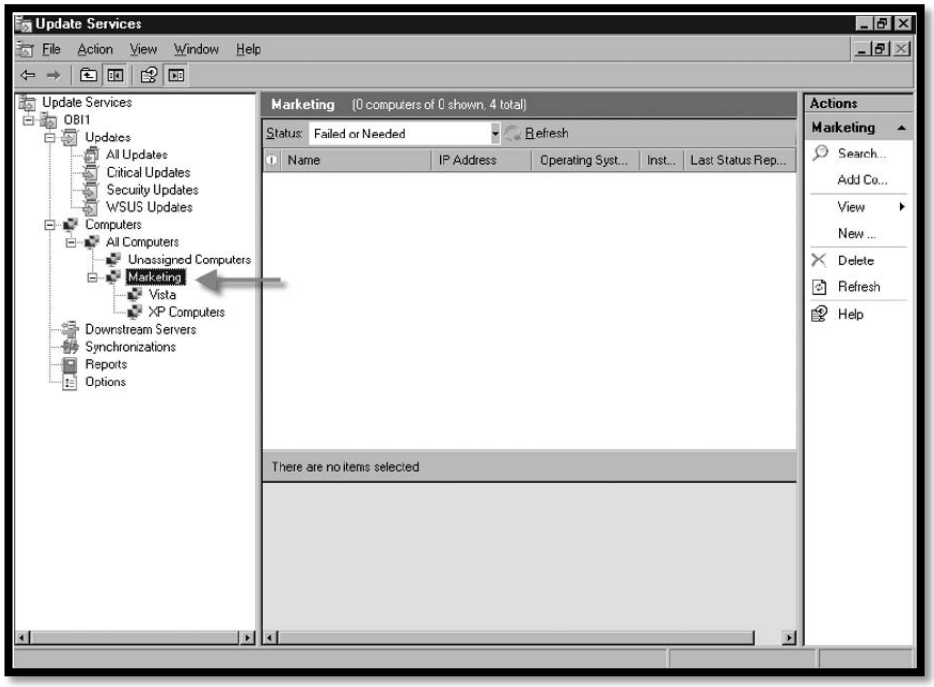


Figura 76: Representa el nodo computers donde se puede ver una posible organización de computadoras.

3.3 Microsoft Operation Manager (MOM) 2005.

Es la herramienta de administración de eventos y rendimiento para Servidores y aplicaciones (Algunas de Terceros) que ayuda a las empresas a reducir el costo y la complejidad asociada con la administración de la infraestructura de red. MOM 2005 permite a los administradores de TI ver y monitorear los servidores y las aplicaciones desde un repositorio central que se alimenta de los miles de eventos y reportes que generan los servidores en la red evitando que ciertos eventos recurrentes pasen desapercibidos y así se pueda tomar una solución planificada. MOM 2005 facilita la administración de eventos de la siguiente forma:

- Simplificado la identificación de problemas de IT. Permitiendo su evaluación y solución posterior.
- Modernizar el proceso de investigación de las causas de un problema facilitando encontrar la raíz de un problema.
- Automatizar una rápida resolución de restauración de servicios y prevención de problemas potenciales de IT.
- Incrementar la efectividad y el nivel de servicio en IT sin necesidad de aumentar costos.

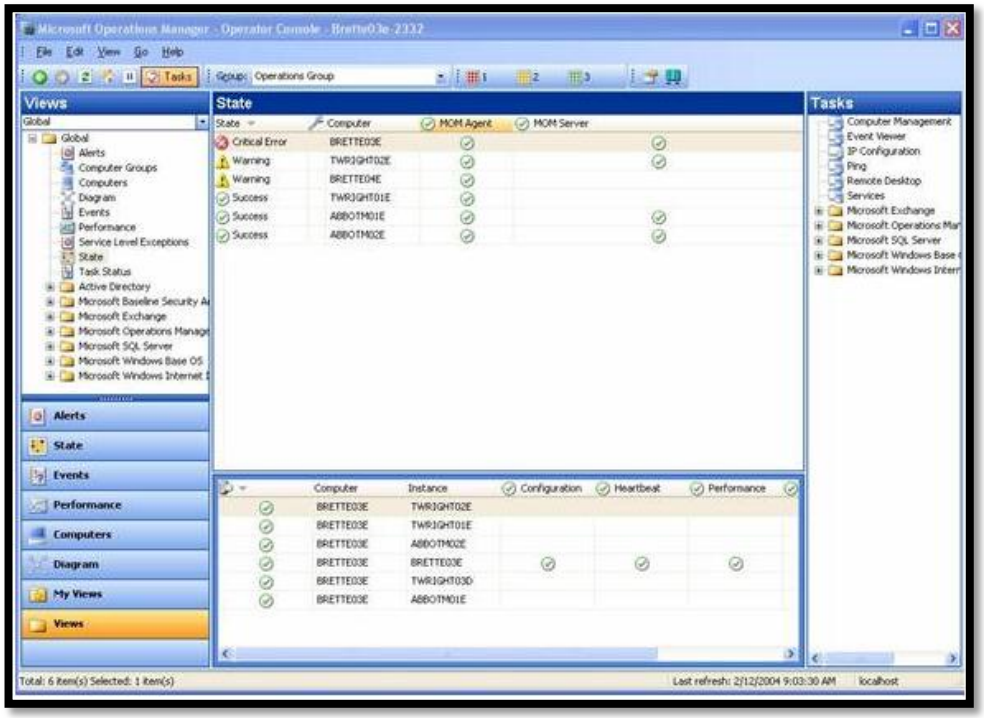


Figura 77: Muestra la vista de las alertas en la consola central MOMO 2005 y la información disponible para las alertas. **Fuente:** http://www.microsoft.com/spain/mom/info/mom2005

Capítulo 4. Implantación de FCS en el LTIC de la Facultad de Ingeniería.

Antes de la implantación de cualquier software que podría afectar el desempeño de los computadores de red. Se debe considerar muchos factores mismos que se deben configurar de acuerdo a los requerimientos de cada organización porque es verdad que existen configuraciones generales pero también deben cumplir con las normas que cada organización disponga en su red. Entre los factores a tomar en cuenta están:

- **Los recursos de hardware:** Los servidores y estaciones de trabajo disponibles. Si existe la posibilidad de ambientes de pruebas. De acuerdo a esta información se podrá determinar la topología a implantarse.
- **Los recursos de software:** La existencia de soluciones complementarias o de terceros. Otro aspecto importante es el costo de licenciamiento. La existencia de convenios como Software Assurance de Microsoft el cual cubre un costo anual y permite utilizar cualquier software o licencias del tipo estudiantil que se pueden utilizar a nivel educativo.
- **Las políticas de empresa:** Tener entrevistas con el administrador de la red para conocer cuáles son las necesidades y que controles son factibles de tomar en cuenta ya que un nivel muy controlado puede en ciertos casos no ser de gusto para la organización es decir se debe realizar una implantación de acuerdo a los requerimientos mediante un consenso con el administrador o personal administrativo a nivel de gerencia.

4.1 Estudio del LTIC de la Facultad de Ingeniería.

El LTIC, es una unidad de servicios de la facultad de ingeniería de la Pontificia Universidad Católica del Ecuador. Este administra los equipos, programas y otras tecnologías

relacionadas con información y comunicación de la facultad mencionada. Actualmente ocupa todo el segundo piso del edificio de la facultad.

Los servicios y funciones que tiene el LTIC. Son la colaboración con el cuerpo docente y estudiantes en las actividades prácticas relacionadas con tecnologías de información, así mismo ayudan al desarrollo e investigación en las áreas de TI y computación.

El LTIC. Capacita a docentes, administrativos, becarios, ayudantes y estudiantes de la facultad de ingeniería en las áreas de TI. Además de ofertar servicios y asesorías a otras Unidades Académicas de la PUCE en la concerniente a TI, brinda servicios a terceros bajo las normativas de la PUCE

Debido a la importancia de sus servicios el laboratorio no puede caer víctima de ataques de software malicioso que afecten su desempeño o peor aun dejar de prestar sus servicios.

Pero mantener un ambiente seguro en un laboratorio donde los usuarios en su totalidad son estudiantes de ingeniería en sistemas así como también los estudiantes de ingeniería civil, plantea un reto mayor al administrador de red porque son personas con mayores conocimientos en relación de un usuario común de cualquier organización. Así plantear una estrategia de seguridad que se ajuste a este nivel de usuarios es mucho más complicado, demandando del administrador un mayor control y conocimiento de los sistemas que utiliza para este objetivo.

Enfocándose en los recursos disponibles para efectuar la implementación del sistema de gestión central y unificado de seguridad. Se debe tomar en cuenta el hardware como estaciones de trabajo en cada aula, servidores disponibles y la red que dispone el laboratorio. Y el software instalado en cada estación de trabajo.

- **Hardware:** Existe un gran número de estaciones de trabajo funcionando en el laboratorio lo cual plantea un problema de administración igual de complejo que en

una organización. Las estaciones de trabajo tienen funcionando gran cantidad de programas destinados al aprendizaje de la programación por tanto las políticas de grupo y el software antivirus a utilizar no debe afectar el desempeño de los mismos.

- **Software:** El sistema operativo base es Windows XP Professional, en todas las estaciones de trabajo al igual que en muchas organizaciones sigue siendo el sistema operativo preponderante por su estabilidad y bajo consumo de recursos en relación de versiones más posteriores como Windows Vista o Windows 7. Para mantenerse desapercibido para los usuarios el software antivirus aparte de mantener protegido el sistema debe tener un bajo perfil en consumo de recursos ya que los recursos de la estación de trabajo deben estar enfocados en los programas educativos mas no solo en la seguridad.
- **Servidores:** Los servidores son de vital importancia en la implementación de un sistema de seguridad unificado, debido a que este tipo de sistemas requiere de algunos servidores en ciertos casos. Para tomar ventaja del hardware de los servidores el cual podría verse como desperdiciado al utilizarlo solo como un servidor de dominio. Se tomó la dación de utilizar tecnología de virtualización.

  La cual ya estaba disponible en el servidor principal con Windows Server 2008 Hyper-V.
- **Tecnología de virtualización (Hyper-V):** Diseñada por Microsoft la cual permite virtualizar todo tipo de sistemas operativos Windows e incluso sistemas operativos de terceros como los basados en Linux. Mediante esta tecnología se puede instalar en un solo servidor físico varios otros servidores tantos como la tecnología de virtualización permita en relación de los recursos del servidor físico.

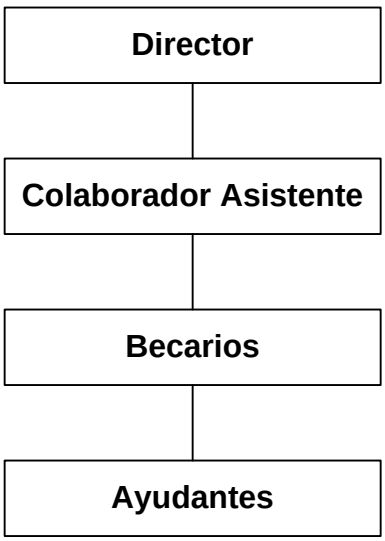


Figura 78: Organigrama de funcionarios y personal en el LTIC de la facultad de ingeniería de la PUCE.
Fuente: Laboratorio LTIC.

El director del LTIC: Se responsabiliza de supervisar el correcto funcionamiento de la infraestructura del laboratorio además de la delegación de funciones.

El colaborador – asistente: Se encarga de la logística del laboratorio y soluciones de software libre dentro del mismo del licenciamiento de software comercial entre otras tareas.

Los becarios: Son los estudiantes seleccionados para trabajar directamente con las actividades del LTIC trabajan directamente en los proyectos y actividades delegadas por el director o el colaborador – asistente.

Los ayudantes: también son estudiantes pero son utilizados como apoyo a los becarios en otras actividades de menor prioridad.

4.1.1 Infraestructura LTIC.

La infraestructura (Tomada Noviembre del 2009), es muy importante antes de realizar cualquier implementación de software que va a ser instalado en cada estación de trabajo porque de acuerdo a los sistemas operativos instalados en estaciones y servidores se

deberá reconocer que requisitos son los faltantes para ser debidamente actualizados con los requisitos mínimos del software planeado a implementar. El hardware con su respectivo software se lista a continuación:

Estaciones Servidores:

Sala Servidores			
Modelo	**HP Power Edge 2950**	**HP Power Edge 2950**	**HP Power Edge 2950**
Cantidad	2	2	1
Procesador	Intel ® Xeon X5355 2.66 GHZ (4 Núcleos)	Intel ® Xeon X5355 2.66 GHZ (4 Núcleos)	Intel ® Xeon X5355 2.66 GHZ (4 Núcleos)
RAM	4 Gb	8 Gb	4 Gb
DISCO	67.7 Gb / 100 Gb	100 Gb / 136 Gb	67.7 Gb / 100 Gb
Disquetera	No	No	No
CD/DVD	Si	Si	Si
Tarjetas de Red	2	2	2

Tabla 4: Tabla de equipos sala de servidores LTIC.
Fuente: Hugo Paredes

Estaciones Clientes:

Aula 201			
Modelo	**AOPEN**	**Hp dc5000**	**Compaq d31vm**
Cantidad	5	7	2
Procesador	Pentium IV 2.4 GHz	Pentium IV 3,0 GHz	Pentium IV 1,8 GHz
RAM	512 MB	512 MB	512 MB
DISCO	40 GB	40 GB	40 GB
Disquetera	si	si	si
CD/DVD	CD ROM	CD ROM	CD ROM
USB	4 posterior	2 frontales, 4 posteriores	2 frontales, 4 posteriores

Tabla 5: Tabla de equipos aula 201 LTIC.
Fuente: Hugo Paredes

Infraestructura LTIC

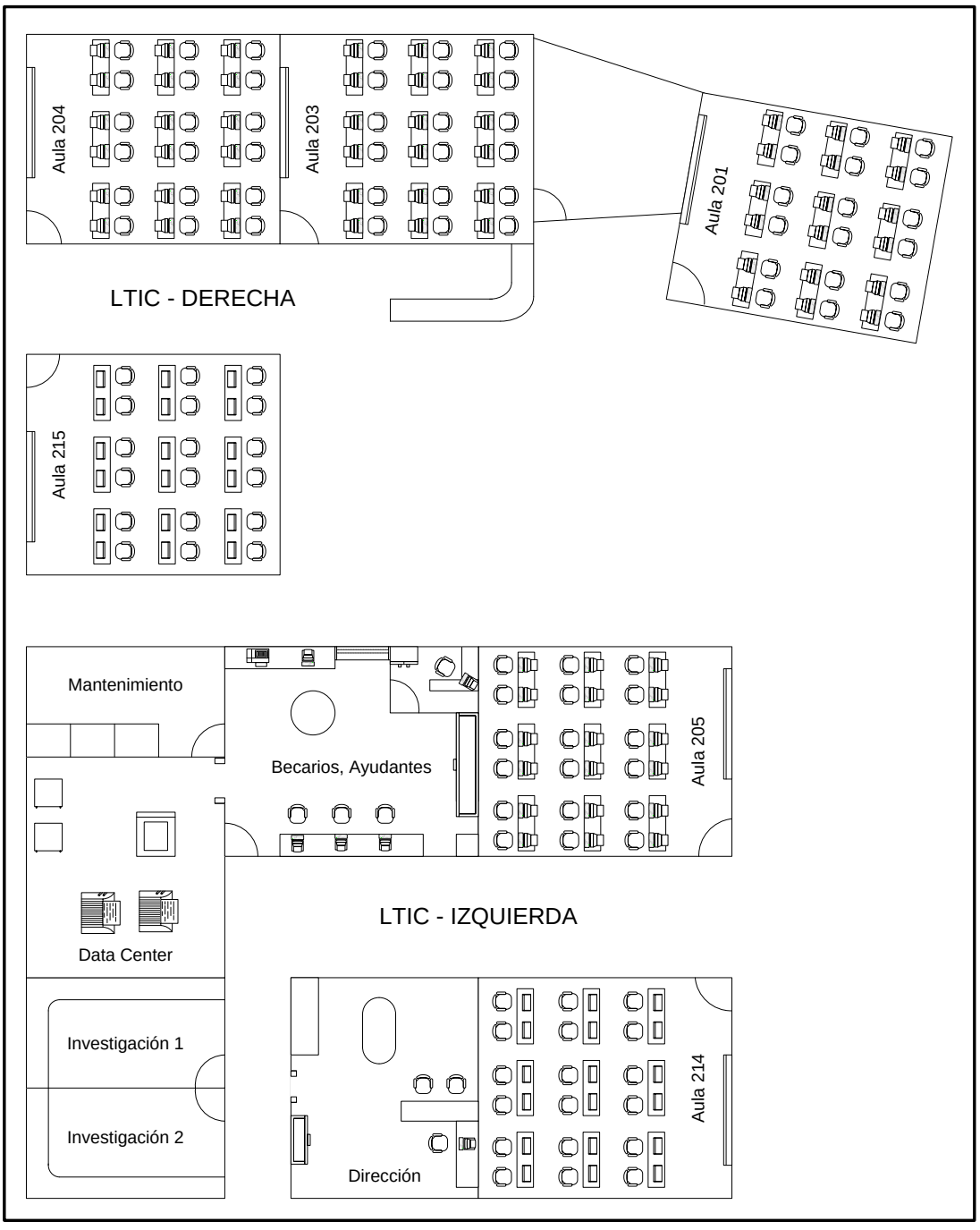


Figura 79: Diseño del LTIC Facultad de Ingeniería de la PUCE.
Fuente: Laboratorio LTIC.

4.1.2 Sistemas Operativos.

El LTIC posee como base principalmente sistemas operativos Microsoft listados a continuación:

Estaciones Cliente.

- Microsoft Windows Service PACK 2 Español
- Microsoft Windows Service PACK 3 Español

Servidores Físicos.

- Windows Server 2003 SP Español
- Windows Server 2008 SP2 Español
- Windows Server 2008 R2 Español

Servidores Virtualidados (Hyper-V)

- Windows Server 2003 R2 Español Servidor de dominio, Consola de gestión central y unificada Forefront Client Security (FCS).

Requerimientos		
Sistema Operativo Cliente	**Disco Duro**	**Memoria**
Windows XP Professional	2 Gb	126Mb
Windows Vista	5 Gb	512Mb

Tabla 7: Requerimientos mínimos de versiones de sistemas operativos clientes.
Fuente: Hugo Paredes

4.1.3 Soluciones de seguridad.

La LTIC posee dos protecciones principales las cuales son el software antivirus (NOD 32) y un firewall a nivel de software (Untangle) con los cuales hacen frente a las amenazas de software malicioso u otros ataques fraudulentos. Pero debido al flujo de estudiantes y docentes que utilizan las aulas del laboratorio se hace muy difícil detectar a tiempo epidemias de virus ocasionadas por computadoras vulnerables y tomar acción inmediata es imposible debido a que la protección antivirus actual funciona de forma independiente en cada computador.

- **Antivirus Nod32 v3 ESET:** Nod 32 es un software antivirus que tiene buena aceptación y es conocido como un buen antivirus. Pero el software antivirus utilizado en computadores personales no debería ser utilizado en la misma forma en las computadoras de una organización porque cada antivirus actúa como isla es decir no existe comunicación alguna entre estaciones. Aunque una solución antivirus de este tipo si puede ser direccionada a un repositorio de actualizaciones no es la forma óptima de manejar las actualizaciones porque este proceso es manual y no permite conocer que computadoras no pueden conectarse para recibir las actualizaciones.
- Este tipo de software antivirus también tiene la cualidad de indicar que tipo de actualizaciones de seguridad tiene el computador pero no tiene la capacidad de descargarlas y genera otro problema al administrador de la red ya que debería realizar una instalación manual en cada estación lo cual se podría realizar pero resulta ilógico cuando son un gran número de estaciones y se pueden configurar repositorios como el WSUS.
- El gran problema de utilizar este tipo de protección es el monitoreo que no se facilita para el administrador de la red quien debería realizar mucho trabajo manual para

obtenerla así como actuar de forma oportuna y a la vez en todas las estaciones de la organización.

- De ahí la importancia de manejar software que permita una administración centralizada donde se pueda monitorear, descargar actualización y actuar en contra de amenazas de software malicioso.

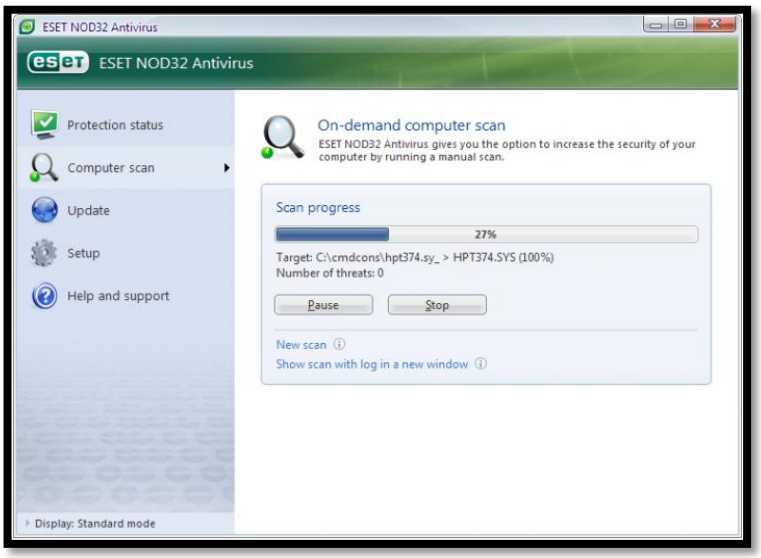


Figura 80: Antivirus cliente NOD 32 versión 3 configurada en los computadores clientes del LTIC.

Firewall Untangle: Es una empresa privada que ofrece una solución de seguridad de red firewall (network gateway) de código abierto para pequeñas empresas. Untangle ofrece muchas aplicaciones que ayudan a controlar la seguridad de la red como:

- Bloqueo de correo electrónico del tipo spam.
- Bloqueo de software malicioso malware.
- Filtrado de web.
- Protección contra robo de información sensible phishing.
- Prevención de intrusiones externas.

Untangle como cualquier otra solución firewall es de vital importancia en una organización porque es el primer escudo defensivo en contra de ataques maliciosos. Es una parte del sistema de seguridad que ya tenía implantado el LTIC.

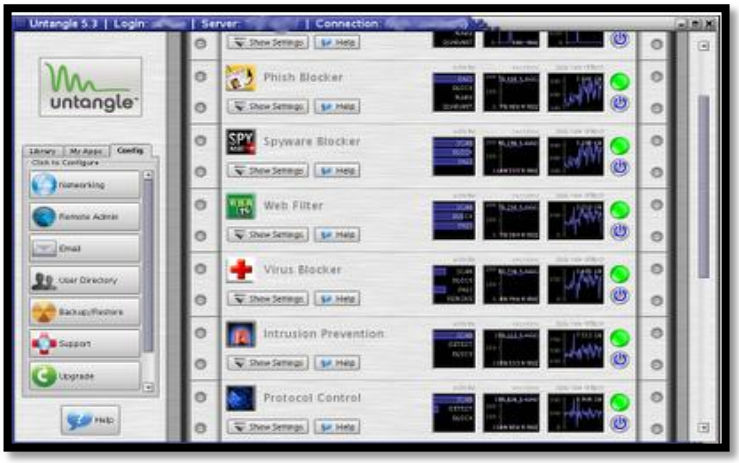


Figura 81: Consola principal Untangle. Solución de seguridad firewall del LTIC.

4.1.4 Tipos de licenciamiento Microsoft.

Paquete de producto completo (FPP, Full packaged product): Puede adquirir software de Microsoft empaquetado para la venta en comercios o centros distribuidores. Esta opción solamente resulta apropiada para usuarios que requieren copias individuales de productos de Microsoft.

Fabricantes de equipos originales OEM: El software de Microsoft se proporciona instalado en equipos de escritorio nuevos suministrados por OEM, como fabricantes de PC o desarrolladores de sistemas.

La característica de esta licencia es que nace y muere con la máquina, es decir no es transferible a otra máquina, y debe ser vendida únicamente con un equipo de computación nuevo.

El costo de la licencia debe constar como un rubro más dentro de la factura equipo detallado.

Licenciamiento por volumen: El licenciamiento por volumen proporciona grandes ahorros, ya que solamente se adquiere la licencia de software (derecho de usar un producto o programa) sin medio de instalación, el mismo que puede ser solicitado a un bajo costo por separado, al igual que la documentación y el soporte para el producto.

Generalmente una licencia que se vende en paquete contiene un medio de instalación que un CD DVD, una guía de usuarios, e información acerca de soporte para el producto y los términos de la licencia de software, conocida como el contrato de licencia del usuario final.

MSDN Academic Alliance (MSDN AA): Este acuerdo es un programa de membrecía anual para facultades e instituciones educativas, tales como la ING de sistemas, ciencias computacionales y sistemas informáticos.

La membrecía proporciona una solución accesible y completa para la investigación, permitiendo tanto a docentes como estudiantes tener acceso a las últimas herramientas de desarrollo, sistemas operativos, documentación y referencias técnicas.

4.2 Escenario de implementación FCS en el LTIC de la Facultad de Ingeniería.

Una vez conocido los recursos disponibles en el LTIC, se puede determinar que la topología de un solo servidor es la adecuada porque permite seguir utilizando el servidor de producción mientras se prepara otro servidor que en primera fase será de pruebas, el que alojara los siguientes servicios:

- Servidor de Dominio donde se configuran políticas de seguridad.
- Servidor Forefront Client Security (FCS).

- Servidor Windows Server Update Services (WSUS).

El servicio de virtualización Hyper-V configurable en Windows Server 2008 SP2, permite aprovechar todos los recursos del servidor físico donde se encuentra instalado. Para que en cierta forma no sean desperdiciados solo siendo utilizados como un servidor de dominio.

Para no afectar el desempeño ni las actividades del laboratorio se configuro en primera fase un servidor de dominio paralelo que una vez configurado será el nuevo servidor de producción.

4.2.1 Creación del escenario.

Antes de realizar la instalación de FCS, se debe crear el nuevo servidor de dominio mismo que servirá de base para todo el sistema a implementar. La topología de un servidor a utilizar se representa en la siguiente gráfica:

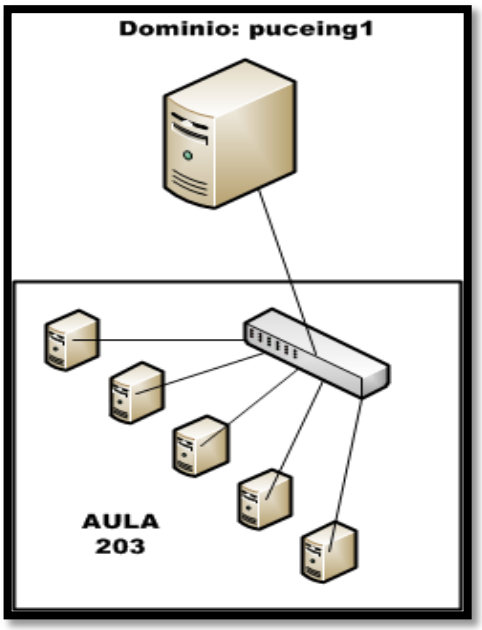


Figura 82: Topología un servidor de dominio y 5 equipos.
Representa el ambiente de pruebas donde se instalara FCS.

El **ANEXO 1** describe en detalle la configuración realizada para levantar la máquina virtual y el dominio PUCEING1.

4.2.2 Creación de políticas de grupo Group Police Manager Console (GPMC).

El principal problema para los administradores es mantener sus estaciones de trabajo siempre funcionales pero es un gran reto mantenerlas así debido a que el administrador no es el responsable directo de todas las fallas o problemas de seguridad que se generan en la red. Muchas de las veces son los usuarios los responsables de estos problemas como ya fue indicado en capítulos anteriores uno de los eslabones más débiles de la cadena de seguridad es el usuario. Entonces mantener una red segura genera un gran reto al administrador de la red debido a que muchas veces su discurso de seguridad informática no es tomado en cuenta o no es entendido por los usuarios los cuales tienen como prioridad su trabajo dejando de lado la idea de mantener segura su estación.

Una de las herramientas puede utilizar el administrador para reforzar estas prácticas automáticamente en cada una de las estaciones de la red es la consola GPMC.

GPMC.

Es una consola de administración que permite manejar las directivas de grupo mediante una serie de plantillas previamente configuradas las cuales ayudan a configurar una variedad de tareas en una única herramienta. Una vez instalada se seguirá utilizando la herramienta de Active Directory para propósitos como crear usuarios, equipos y grupos. Sin embargo GPMC se utilizar para llevar a cabo cualquier tarea relacionada con directivas de grupo. Esta funcionalidad no está disponible en el AD a menos que sea instalada. No significa que el editor de directiva de grupo haya sido reemplazado, puede seguir usándose como antes

solo que GPMC ofrece una funcionalidad de integrada y centralizada de políticas de grupo que utilizan como principal base las llamadas plantillas administrativas.

Plantillas administrativas.

Existen una variedad de archivos de plantillas con la extensión .adm que se incluyen con Windows. Estos archivos son los denominados plantillas administrativas las mismas que proporcionan información de directiva para los elementos que están en la carpeta de Administrative Templates en el árbol dela consola del Editor de directivas. Las plantillas incluyen valores de registro, los cuales se encuentran en la configuración de equipo o usuario en el propio editor.

Una plantilla .adm consiste en una jerarquía de categorías y subcategorías que definen como aparecen las configuraciones de cada directiva. Además, contienen la siguiente información:

- Ubicaciones del registro que corresponden con cada configuración.
- Opciones o restricciones en valores que se asocian a cada configuración.
- Muchas configuraciones poseen un valor predeterminado.
- Exponen una explicación de cada política permitiendo conocer que se realiza al configurarla.
- Las versiones de Windows que son compatibles con cada configuración.

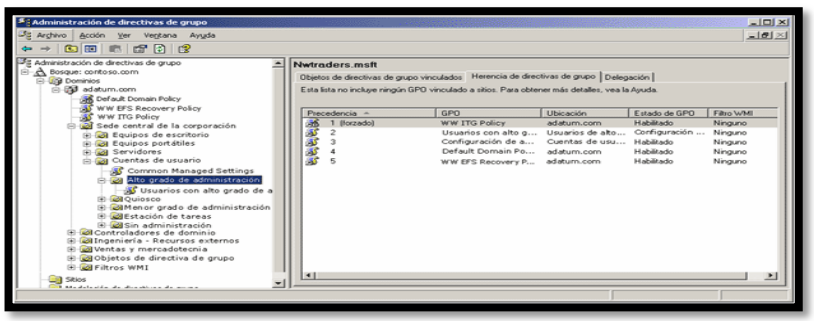


Figura 83: Consola GPMC representa las políticas de grupo y su organización.

No todas las políticas de grupo pueden ser configuradas de la misma forma en todas las organizaciones existen algunas de carácter general que por seguridad se deben habilitar como el auto ejecutar de unidades extraíbles y USB. Pero existen otras como instalación petición de permisos de administrador que ciertos usuarios a nivel de gerente no suelen requerir este requisito. Así que cada configuración a realizar se debe realizar en consenso con el administrador de red y administrativos superiores para mantener la armonía y comunicación entre las partes al mismo tiempo que se mantiene un ambiente seguro.

En el **ANEXO 2** Se especifica cómo realizar la configuración de las políticas en el ambiente del LTIC y cuales fueron tomadas en consideración.

4.2.3 Definición de la topología de Forefront Client Security.

Una vez considerado los recursos disponibles y ya configurando una base segura mediante el uso de políticas de grupo (GPMC). La topología a escoger para la instalación del sistema de gestión central y unificada sobre seguridad en ambientes Microsoft Forefront Client Security. Es la topología de un solo servidor.

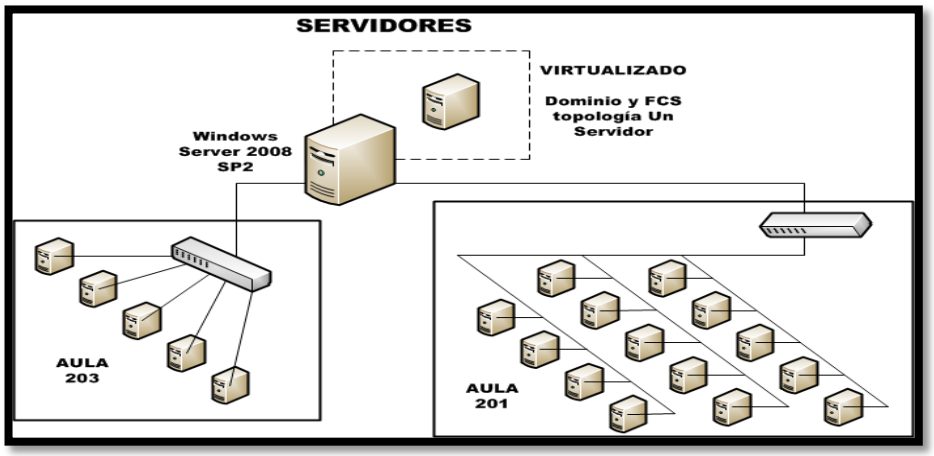


Figura 84: Topología de un solo servidor FCS a implementar en el LTIC.

La topología de un solo servidor permite manejar todos los servicios de FCS en un solo servidor.

Esta instalación de esta topología depende de muchos pasos para su configuración completa las cuales se describen en el **ANEXO 3**.

4.2.4 Definición de la topología de Windows Server Update Services WSUS.

Debido a que no existe un servidor WSUS presente en el LTIC, se tomara como base el único servidor presente en la topología FCS de un solo servidor. Esta topología es fácilmente configurable y soportable porque no hay una gran cantidad de computadores en relación de todos los computadores que pueden soportar la topología de un solo servidor. Así el servidor WSUS con su topología de un solo servidor es de fácil configuración y de gran ayuda para los recursos disponibles.

La configuración de la topología WSUS de un solo servidor no es de gran complejidad pero donde se encuentra es la decisión de que actualizaciones descargar y cuales instalar en las estaciones para evitar problemas a futuro.

En el **ANEXO 4** se describe su instalación, configuración de políticas y decisiones de instalación a aprobar.

4.2.5 Monitoreo y gestión de la consola FCS.

Una vez instalado y configurado cualquier sistema presenta un nuevo desafío para el administrador de red el cual es aprender a utilizar la nueva herramienta para que la misma sea de ayuda en sus entorno de red y no solo termine con una herramienta más que otra empresa o técnico dejo configurada siendo simplemente dejada en el mismo estado como

fue entregada. Toda herramienta nueva puede ser de ayuda o no es decisión del administrador de red quien deberá monitorear y gestionar el nuevo software.

La consola FCS es una consola de fácil aprendizaje en relación de otras consolas como la de McAfee la cual necesita mucho más entendimiento de la misma y en muchos casos se termina siendo dependiente de la empresa quien la configuro para realizar cambios mayores los cuales son los de mayor importancia en relación de solo realizar una consulta u actualización de definiciones de virus en la consola central.

En el **ANEXO 5** se describe los procedimientos de instalación de agentes, monitoreo de computadores, lectura de informes, configuraciones de políticas de seguridad, etc. En relación todo lo referente a la administración de la consola FCS.

4.3 Situación actual y soluciones.

La situación actual del LTIC no es diferente a la de muchas instituciones o empresas. Es decir existe conciencia en la importancia de mantener una red segura, estaciones funcionales y libres de virus, controles de acceso a internet y mantener el control en las estaciones a nivel de administrador para cambios en configuraciones. Aunque cada administrador de red conoce la importancia de la seguridad no siempre puede mantener la seguridad de su red en un nivel verdaderamente configurado a los estándares más óptimos.

Esto es debido a que no todas las organizaciones tienen el suficiente presupuesto para invertir en opciones de seguridad o mantener personal especializado que se encargue de la seguridad en la red ya que la mayoría administradores de red tienen que convertirse en una suerte de hombre orquesta quien se encarga de todos las funciones desde la programación, administrar la red, realizar help desk en toda la organización y varias tareas de seguridad en la red la cual es tomada en cuenta solo cuando ocurren ataques de software malicioso que afectan el desempeño de la red de la organización.

Entre los problemas de seguridad comunes entre los cuales también se encuentran los del LTIC están:

Políticas de grupo.

No toda la seguridad de la red es controlada por software antivirus o los firewalls dispuestos en la red. Otro gran aliado de la seguridad son las políticas de grupo, pero existe un gran problema y es que no todos los administradores de red tienen experiencia en el manejo de servidores a nivel de la creación de las políticas de grupo, debido a esto no son configuradas políticas para controlar la seguridad red.

Así no son configuradas políticas que en muchos de los casos son de rápida configuración pero que se reflejan en un gran aumento en seguridad como por ejemplo:

- **Deshabilitar el AUTORUN de los CD, DVD y dispositivos extraíbles como memorias USB** (Aunque la configuración de la política de grupo para deshabilitar esta opción es relativamente rápida es muy común que no sea desplegada y debido a la facilidad de adquirir un dispositivo USB la mayoría de los virus utilizan esta falla de seguridad para infectar los equipos).
- **Evitar el acceso al panel de control** (Aunque ciertas organizaciones evitar tener esta configuración es una buena recomendación mantenerla activa debido a que en este menú se pueden realizar varias modificaciones que actúan directamente con la estabilidad del computador como el firewall, puntos de restauración, etc.).
- **Evitar el acceso al símbolo de sistema** (Es una de las políticas que debería ser configurada siempre debido a que mediante este acceso se puede realizar configuraciones vía línea de código evitando la seguridad de permisos como los de administrador. Aunque para realizar configuraciones en esta vía se necesitan personas más capacitadas en ese tema siempre se puede dar ese caso).

- **Evitar el cambio de papel tapiz** (Aunque puede parecer algo más estético es importante para mantener un estándar incluso subiendo fotos de la organización o propagandas para el conocimiento del personal. Pero la importancia de esta política es debido a que existen muchos usuarios que suelen subir fotos inapropiadas y con frecuencia en un ambiente de estudiantes).
- **Evitar acceso a la configuración de redes** (Es otra media importante así se evita que se cambie direcciones IP o puedan conocer si se utilizan direcciones fijas o DHCP. Porque si se utiliza control vía IP de acceso al internet con el solo cambio de esta configuración podrían saltarse esta seguridad).
- **Ejecutar instaladores con permisos de administrador.** (Esta configuración es de vital importancia en cualquier organización para mantener solo el software que el administrador de red desea en las estaciones de trabajo y así evitar que software sin el debida prueba o aprobación sea instalado como programas de descarga de música, videos, reproductores de música, barras para Internet Explorer. Las cuales pueden dañar el correcto desempeño de la estación de trabajo y después el administrador de red tiene que reparar el equipo por daños que podían ser evitados).
- **Desconfigurar los puntos de restauración** (Es otra política importante para evitar la contaminación de virus porque los mismos pueden ser eliminados en la sesión activa pero seguir activos en un punto de restauración anterior es decir si se restaura el equipo puede volver a infectar el equipo y la red).
- **Configurar las actualizaciones en el servidor centralizado** (La actualizaciones deben ser canalizadas en un repositorio centralizado como WSUS para evitar que la red se congestione con tráfico de actualizaciones y mantener una red con clientes actualizados).

En relación existe una gran cantidad de políticas de grupo configurables pero siempre dependen de las necesidades de la organización y la ambiente donde se encuentra el directorio activo configurado. Las políticas de grupo son un gran aliado para mantener la seguridad en la red.

Servidor centralizado de actualizaciones.

Uno de los mayores problemas con la administración de una red es mantenerla actualizada por la gran cantidad de actualizaciones de seguridad que suelen ser necesarias con el paso del tiempo en los sistemas operativos.

Así configurar un repositorio centralizado o servidor de actualizaciones como el configurado Windows Server Update Services WSUS, ayuda a:

- **Mantener la red actualizada:** Ya que el servidor se sincroniza y descarga las actualizaciones de seguridad requeridas para la red. Están ahora disponibles en un servidor en la red local ayudando a mantener la red actualizada evitando disminuir el ancho de banda de internet al conectarse todos los clientes el sitio de actualizaciones de Microsoft (Windows Update).
- **Controlar las actualizaciones:** Las actualizaciones y parches de seguridad no deben ser desplegadas apenas son descargadas porque las mismas pueden causar problemas en aplicaciones de la organización. Así mediante la creación de grupos de clientes en el servidor WSUS, se pueden descargar e instalar las mismas de forma controlada evitando afectar toda la red en caso que una actualización afecté el desempeño de los clientes.

Sistema de gestión central y unificada sobre seguridad en ambientes Microsoft.

Una consola centralizada de administración de seguridad es importante para ayudar en la administración de la seguridad de la red. Debido a que existen muchos aspectos a tomar en cuenta para que la red sea realmente segura.

La consola de administración centralizada Forefront Client Security FCS, ayuda al administrador a mantener la red segura. Mediante el uso de un cliente antivirus centralizado, servidor de actualizaciones centralizado e información centralizada del estado de seguridad de la red.

- **Cliente antivirus centralizado FCS:** Un cliente antivirus corporativo es importante para mantener un red segura porque los usuarios no tienen la misma conciencia de seguridad en un pc de empresa o educativo que en su computador personal, es decir un estudiante no le interesa pasar el antivirus a su dispositivo USB al usar el pc de su unidad educativa porque no es un pc propio. El cliente antivirus debe ser configurado de forma centralizada para que realice escaneos programados sin necesidad de que el usuario ocasional lo realice.
- **Servidor centralizado de actualizaciones:** La consola de FCS se complementa directamente con el servidor WSUS porque son consolas creadas por Microsoft, es decir se complementan de forma nativa.
- **Información centralizada:** Debido a que la solución actual solo maneja actualizaciones centralizadas. No ofrece ninguna información centralizada referente a los casos de malware detectado, estado de seguridad, tipos de ataques. Aunque esta información está disponible en el antivirus al no ser un solución corporativa no está centralizado su manejo es decir son islas que no pueden ser configuradas ni mostrar ninguna información acerca del estado en la red.

Por ejemplo: Este momento si un virus ataque solo sabremos que ataco o fue limpiado pero no podremos atacar la raíz de la contaminación porque no tenemos ninguna información acerca del equipo que fue la fuente del ataque así como los parches necesarios para evitar que el virus se descargue por toda la red.

Aunque existe una solución firewall que también escanea la red y provee alguna información la cual no es accesible debido a que la solución que almacena captura esta información termino con su periodo de prueba y ya no proporciona ninguna información.

Virtualización.

Hyper-v proporciona una plataforma ideal para los principales escenarios de virtualización, como la consolidación de servidores en producción, continuidad del negocio, pruebas y desarrollo de software, así como escalabilidad, alto rendimiento, fiabilidad, seguridad, flexibilidad y capacidad de administración.

La flexibilidad y la capacidad de una rápida migración de las máquinas virtuales de un equipo físico a otro a través de clusters o dispositivos externos de almacenamiento. Permiten seguir la continuidad de los servidores con una pequeña ventana de tiempo al cambiar de servidores físicos.

Ejemplo: El LTIC utiliza la capacidad de virtualización del server 2008 Hyper-v esto permite mantener respaldos de los servidores de producción en caso de perder capacidad en un servidor físico. Es decir se pueden pasar las máquinas virtuales de un servidor a otro.

Conclusiones.

Todo administrador de red tiene conciencia de la importancia de la seguridad informática en su organización para mantener una infraestructura segura. Conocen de la existencia de procedimientos y herramientas necesarias para cumplir con ese objetivo. Pero es común que no sean aplicados estos conceptos aunque exista la documentación y el acceso a la tecnología adecuada.

Falta de personal especializado, ya que es común que el administrador de red en varias ocasiones tenga la responsabilidad de conocer de todo, es decir de infraestructura, bases de datos, programación, atención help desk, etc. Sumado a problemas de falta de presupuesto para adquirir nueva tecnología de seguridad o actualizar la existente, combinado al desconocimiento de administración de la tecnología existente en la organización ya que se depende de la empresa que brindo los servicios de configuración para la resolución de problemas que podrían ser fácilmente superables con el solo conocimiento de cierta parte de la administración de la tecnología. Convierte en un verdadero desafío al administrador de red encontrar soluciones y planificar sus estrategias para mantener su infraestructura segura.

Pensar que se tiene asegurada la red con el solo hecho de adquirir el software antivirus de última generación con la última actualización del día es un grave error. Porque la seguridad de la red depende de muchos factores que deben ser analizados en cada organización para determinar cuáles son las prioridades, es decir no se puede manejar las mismas políticas de seguridad en una institución educativa o en empresas con redes relativamente pequeñas que en una organización que maneja información muy sensible como un banco donde no se puede ser permisivo ya que sus controles deben ser muy estrictos.

El software antivirus no es la solución final para mantener la red segura porque se necesita primero tener: una base segura es decir todos los sistemas operativos debidamente actualizados, configurar políticas de grupo vía directorio activo en el caso de redes Microsoft, un software antivirus corporativo que permita administración remota y que proporcione reportes del estado de seguridad de la red, un repositorio de actualizaciones centralizado. Finalmente apoyarse con tecnologías complementarias como el uso firewalls que son el primer filtro contra el software malicioso e intrusiones fraudulentas.

La falta de investigación o lectura de noticias de seguridad informática con problemas de ataques de maliciosos actuales son también otro factor que atenta contra la seguridad de las redes. Porque muchas de las epidemias de virus más grandes se debieron a que los administradores de red no actualizaron a tiempos sus sistemas operativos, ya que si citamos como ejemplo el caso del virus CONFICKTER solo era necesario descargar un parche de seguridad de unos pocos kilobytes para evitar que este virus tan persistente y peligroso ataque la red.

El problema con los ataques de software malicioso es que los administradores de red solo suelen tomar acciones al momento que son atacadas sus redes y es cuando realizan las acciones correctivas como actualización de parches de seguridad, se buscan nuevas soluciones de software antivirus, se crean planes para eliminar el software malicioso, etc. Pero los administradores de red deberían tomar conciencia como en cualquier problema, que es mejor prevenir antes que caer víctima de estos ataques de software malicioso o fraudulento.

Recomendaciones.

La investigación es una de las mejores acciones preventivas para mantener una red segura. Porque permite al administrador de red conocer sobre soluciones actuales contra software malicioso o conocer si con solo unas pocas configuraciones en sus servidores pueden mejorar la seguridad de su red.

Por ejemplo: La configuración de una política de grupo que evite la auto ejecución de CDs, DVD o dispositivos extraíbles, puede mejorar en gran medida la seguridad de la red, ya que muchos de los virus explotan esta opción para ejecutarse una vez que se conectan al computador.

Realizar una auditoría de seguridad mediante el uso de programas especializados como sniffers que pueden revelar los problemas de seguridad que tiene nuestra red. Una vez conocidos los problemas de seguridad se pueden crear planes correctivos para solucionarlos. También crear la respectiva documentación de administración de la tecnología de seguridad existente en la organización permite delegar obligaciones a otros colaboradores o evitar problemas al momento que se cambie el personal.

Es importante tener en cuenta que existen soluciones de seguridad para usuarios finales y empresariales. Las cuales no deberían ser utilizadas en plataformas que no corresponden porque un software corporativo permite administración remota, brindando informes de seguridad centralizados. También se debe tener en cuenta que es mucho mejor mantener tecnología que sea complementaria y que sea de fácil administración.

Uno de los servicios que no debería faltar en una red es un reposito de actualizaciones centralizado porque el mismo ayuda con dos principales objetivos, el primero mantener todos los clientes y servidores actualizados. Y segundo objetivo evitar que se desperdicie el ancho de banda de internet por descargas de actualizaciones directamente del internet.

Para las plataformas Microsoft existen varias utilidades que realizan esta actividad pero tienen un costo, así Microsoft libero el servidor Windows Server Update Services de forma gratuita para que los usuarios de plataformas Microsoft mantengan sus infraestructuras actualizadas.

Bibliografía.

Libros Electrónicos.

- **Texto tomado de:** BORGHELLO, Cristian. *Cronología de los virus informáticos: historia del malware*. [en línea].ESET Latinoamérica, 14/11/2006, 4/12/2009, [citado 10-01-2009], Formato pdf, Disponible en Internet: http://www.eset-la.com/press/informe/cronologia_virus_informaticos.pdf.
- **Texto tomado de:** LAWTON, Lynn; JONSON, Robert. *Manual de Preparación al Examen CISA 200* [en línea]. ISACA, 2007, 42008, [citado 10-12-2009], Formato pdf, Disponible en Internet: http://www.isaca.org/cisajobpractice.
- MARTIN, Helen, *Virus Bulletin about us* [en línea]. Virus Bulletin, 2010, [citado 1-2-2010], Disponible en *Internet: http://www.virusbtn.com/about/index*.
- **Texto tomado de:** VARSALONE, Jesse. Microsoft Forefront Security Administration Guide. [en línea]. Windows Security org,1/1/2008, [citado 1-08-2009], Formato pdf, Disponible en Internet: http://www.windowsecurity.com/forefrontclientsecurity/forefront_administrationguide.pdf .

Internet

- **"Preparing to install Client Security",** tomado de: http://technet.microsoft.com/en-us/library/bb404270.aspx, acceso: (01/12/2009).
- **"Forefront Client Security Remote Definitions Update Using MOM Tasks",** tomado de: http://blogs.microsoft.co.il/blogs/yanivf/archive/2008/06/09/forefront-client-security-remote-definitions-update-using-mom-tasks.aspx, acceso: (01/12/2009).

- **"Installing Microsoft Forefront Client Security",** tomado de: http://smartquys.wordpress.com/2007/06/02/installing-microsoft-forefront-client-security/, acceso: (12/12/2009).
- **"Forefront Client Security 1ª Parte : Instalando",** tomado de: http://geeks.ms/blogs/dmatey/archive/2007/05/02/forefront-client-security-1-170-parte-instalando.aspx, acceso: (12/12/2009).
- **"Microsoft Forefront Client Security Product Documentation",** tomado de: http://www.microsoft.com/downloads/en/confirmation.aspx?familyId=90044d88-299b-49fb-b762-eae17a1f01f4&displayLang=en, acceso: (14/12/2009).
- **"Deploying the FCS Client Agent in a Corporate Environment to a Target currently running an unmanaged FCS Client Agent",** tomado de: http://itprosecure.com/blogs/fcs_administration/archive/2009/04/09/forefront-client-security-deploying-the-fcs-client-agent-to-a-target-currently-running-standalone-fcs-client-agent.aspx, acceso: (14/12/2009).
- **"Cómo funciona Forefront Client Security",** tomado de: http://geeks.ms/blogs/jesusgonzales/archive/2007/06/15/c-243-mo-funciona-forefront-client-security.aspx, acceso: (05/01/2010).
- **"Forefront Client Security Deployment Tool",** tomado de: http://blogs.microsoft.co.il/blogs/yanivf/archive/tags/Forefront+Client+Security/default.aspx, acceso: (06/01/2010).
- **"Forefront Client Security: Administración centralizada contra virus y spyware, obtén reportes de vulnerabilidades y alertas en tiempo real",** tomado de: http://blogs.technet.com/seguridadydisponibilidad/archive/2008/05/07/forefront-client-security-administraci-n-centralizada-contra-virus-y-spyware-obt-n-reportes-de-vulnerabilidades-y-alertas-en-tiempo-real.aspx, acceso: (06/01/2010).

- **"Microsoft Forefront Client Security TCO Analysis",** tomado de: http://www.silicon.com/white-papers/intrusion-tampering/2008/06/01/microsoft-forefront-client-security-tco-analysis-60608754/, acceso: (07/01/2010).
- **"Microsoft Forefront Client Security",** tomado de: https://partner.microsoft.com/40029561, acceso: (10/01/2010).
- **"Forefront Client Security KB956280 - Update Issue",** tomado de: http://www.tek-tips.com/viewthread.cfm?qid=1529110&page=3, acceso: (12/02/2010).
- **"Forefront Client Security Alerting and Monitoring",** tomado de: http://social.technet.microsoft.com/Forums/es-ES/Forefrontclientalert/threads, acceso: (14/02/2010).
- **"How to recognize phishing e-mails or links",** tomado de: http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx, acceso: (16/02/2010).
- **"IT security and crime prevention methods",** tomado de: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp, acceso: (20/02/2010).
- **"White Papers",** tomado de: http://www.microsoft.com/Forefront/clientsecurity/en/us/white-papers.aspx, acceso: (29/02/2010).
- **"Microsoft Security Response Center",** tomado de: http://www.microsoft.com/security/msrc/default.aspx, acceso: (01/03/2010).
- **"Microsoft Security Intelligence Report (SIR)",** tomado de: http://www.microsoft.com/security/portal/Threat/SIR.aspx, acceso: (04/03/2010).
- **"Microsoft Security Intelligence Report (SIR) v7",** tomado de: http://edge.technet.com/Media/Microsoft-Security-Intelligence-Report-SIR-v7/, acceso: (05/03/2010).

- **"Adding Computers to WSUS 3.0 SP1",** tomado de: http://www.geekzone.co.nz/chakkaradeep/4564, acceso: (06/03/2010).
- **"HOW TO: Connect Vista to WSUS 3.0",** tomado de: http://apcmag.com/how_to_connect_vista_to_wsus_30.htm#, acceso: (13/03.2010).
- **"Microsoft WSUS Documents",** tomado de: http://www.wsuswiki.com/WSUSDocuments, acceso: (20/03/2010).
- **"WSUS30 Step by Step",** tomado de: http://www.scribd.com/doc/17237533/WSUS30-Step-by-Step, acceso: (28/03/2010).
- **"Configuring WSUS on Client Computers",** tomado de: http://www.cites.illinois.edu/wsus/clientinstall.html, acceso: (30/03/2010).
- **"Install WSUS 3.0 - Step-By-Step",** tomado de: http://blogs.microsoft.co.il/blogs/yanivf/archive/2007/09/23/install-wsus-3-0-step-by-step.aspx, acceso: (30/03/2010).
- **"Update and Configure the Client Computers**", tomado de: http://technet.microsoft.com/en-us/library/cc720520(WS.10).aspx, acceso: (02/04/2010).

Anexos.

Anexo 1. Procedimiento creación y configuración servidor de dominio.

Anexo 2. Procedimiento creación de políticas de grupo.

Anexo 3. Instalación Forefront Client Security FCS.

Anexo 4. Configuración Windows Server Update Services.

Anexo 5. Monitoreo Consola central de administración FCS.