ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Licenciatura en Sistemas de Información

"Análisis de las vulnerabilidades de los servicios de correo Electrónico y Diseño de Soluciones para Controlar estas Vulnerabilidades Informáticas"

TÓPICO DE GRADUACIÓN

Previo a la obtención del título de:

LICENCIADO EN SISTEMAS DE INFORMACIÓN

Presentado por:

PATRICIA PANCHANA MORAN
THELMO ZAMORA BARREZUETA

Guayaquil – Ecuador

AGRADECIMIENTO

Agradezco a Dios por permitirme culminar mi carrera con éxito y guiarme en el camino, a mi madre porque con su ejemplo nos enseñó a mis hermanos y a mi que no hay reto difícil solo basta con proponérselo para lograr lo que se desea, además porque siempre a estado a mi lado apoyándome en todo, a mi familia que me alentaron en todo momento teniendo fe en mi deseo de superación , a mis amigos que estuvieron cerca de mi, a las personas que colaboraron en este proyecto y nos ayudaron en forma directa o indirecta, como también a quienes nos dieron su aporte en lo intelectual y en lo moral, a nuestros profesores que nos dieron parte de su conocimiento y nos guiaron en el transcurso de nuestra laboriosa tesis.

Patricia Panchana Morán

Mi agradecimiento es para Dios por permitirme culminar mis estudios, a mi padre que está en el cielo por todas esas enseñanzas que me sirvieron para enfrentar los desafíos de la vida. A mi querida madre que tanto lucho por este momento y siempre me motivó y me apoyó incondicionalmente. A mi esposa por su compresión y por esas palabras de aliento que me dieron fuerzas para seguir adelante justo cuando más las necesité. A mis queridas hijas por ese tiempo valioso que les quite mientras me dedicaba a estudiar. A mis hermanos por todo su tiempo y cariño, por todo lo que me brindaron muchas gracias a todos.

Thelmo Zamora Barrezueta

DEDICATORIA

A mis padres, mis hermanos, familiares y amigos por estar siempre presente en todo momento sean estos buenos o malos, para ellos este logro en mi vida profesional comprometiéndome que no será el último.

PATRICIA PANCHANA MORÁN

A mis hijas, mi esposa, mis padres, hermanos y amigos por alentarme no dejándome caer en momentos de flaqueza y animándome para salir con éxito de todos los retos que me he propuesto.

THELMO ZAMORA BARREZUETA

TRIBUNAL

Ing. Mónica Villavicencio
Presidente del Tribunal

Ing. Albert Espinal
Director del Tópico

Ing. Lorena Caló
Miembro del Tribunal

Ing. Jaime Lucero
Miembro Principal

DECLARACION EXPRESA

La responsabilidad por los hechos, ideas y doctrinas expuesto en este proyecto, nos corresponden exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior politécnica del Litoral.

(Reglamento de Exámenes y Títulos Profesionales de la ESPOL) .-

Patricia Panchana Morán

Telmo Zamora Barrezueta

RESUMEN

El constante avance tecnológico y el crecimiento de la mensajería electrónica como medio de comunicación y la amenaza que representan los distintos virus, caballos de Troya, gusanos, el correo no solicitado y una variada cantidad de potenciales amenazas en contra de la seguridad de las empresas, requieren de estrategias y técnicas enérgicas para evitar las violaciones de la seguridad y protegernos contra ellas.

Nuestro objetivo principal es garantizar la integridad de los mensajes de correo electrónico e impedir los ataques de seguridad mediante ésta vía implementando una solución de filtrado de mensajes.

En la primera parte de este documento se especifican el análisis de vulnerabilidades a las que están expuestos los sistemas de correo electrónico y los fundamentos teóricos y técnicos que van a permitir el desarrollo de una solución de protección contra los virus en el correo Electrónico. Posteriormente se realiza el Diseño y la presentación de los pasos que se siguieron para la implementación de una solución de protección de nuestro sistema de mensajería utilizando tecnología de punta y basada bajo el esquema de un mail gateway.

INTRODUCCION

Frente a los avances tecnológicos como es el "Internet", la imprescindible necesidad de las empresas de comunicarse por ésta vía. y con el correo electrónico sólidamente establecido como la aplicación clave de las empresas modernas. Es importante considerar diversas medidas de protección para mantener la privacidad e integridad y sobre todo garantizar la seguridad en el correo electrónico.

A continuación presentamos nuestro trabajo que fue diseñado con la finalidad de brindar una solución eficiente de protección del correo electrónico por medio de un Mail Gateway para SMTP.

1. VULNERABILIDADES DE LOS SERVICIOS DE CORREO ELECTRÓNICO 1

1.1 El Correo Electrónico 1

1.1.1 Definición 1

1.1.2 Historia del correo electrónico 1

1.1.3 Ventajas que ofrece el correo electrónico 3

1.2 Estructura de un mensaje de Correo Electrónico 6

1.3 Direcciones de Correo Electrónico 7

1.4 Archivos asociados a los mensajes electrónicos 9

1.5 Protocolos de Correo Electrónico 10

1.5.1 Historia de los protocolos de correo 10

1.6 Clasificación de protocolos de correo 12

1.6.1 Protocolos de transporte de correo 12

1.6.1.1 El protocolo SMTP 12

1.6.1.2 Modelo de comunicaciones SMTP 13

1.6.2 Protocolos de acceso a correo 14

1.6.2.1 Protocolo POP 15

1.6.2.2 Modelo de comunicaciones POP 15

1.6.2.3 IMAP 17

1.7 Clasificaciones de los programas de correo 18

1.7.1 Agente de transferencia de correo 19

1.7.2 Agente de entrega de correo 20

1.7.3 Agente de usuario de correo *20*

1.7.4 Arquitectura y Servicios *21*

1.8 VULNERABILIDADES DE CORREO ELECTRÓNICO 22

1.8.1 ¿Qué es una vulnerabilidad? *22*

1.8.2 ¿Qué es una vulnerabilidad de correo? *24*

1.8.3 Vulnerabilidades de correo electrónico por contenido HTML *24*

1.8.4 Amenazas de los sistemas de Correo *25*

1.8.5 ¿Qué es un Virus? *25*

1.8.6 Principales características de un virus informático *26*

1.8.7 Clasificación de los virus *26*

1.8.7.1 Caballos de Troya 27

1.8.7.2 Camaleones 27

1.8.7.3 Virus polimorfos o mutantes 28

1.8.7.4 Virus sigiloso o stealth 29

1.8.7.5 Retro-virus o Virus antivirus 29

1.8.7.6 Virus multipartitos 30

1.8.7.7 Virus voraces 30

1.8.7.8 Bombas de tiempo 30

1.8.7.9 Macro-virus 31

1.8.7.10 Gusanos 31

1.8.8 ¿ Qué es SPAM ? *32*

1.8.9 Técnicas SPAM *33*

1.8.9.1 Obtención de direcciones de correo 33

1.8.9.2 Envío de los mensajes 34

1.8.9.3 Verificación de la recepción 35

1.8.9.4 Troyanos y ordenadores zombis 35

1.9 ALTERNATIVAS PARA CORREO ELECTRÓNICO SEGURO 35

2. EVALUACIÓN DE DIFERENTES SISTEMAS OPERATIVOS DE RED Y SU IMPACTO ANTE LOS VIRUS 38

2.1 SISTEMAS OPERATIVOS DE RED 38

2.1.1 Introducción 38

2.1.2 Definición de sistema operativo de red 40

2.1.3 Características de un sistema operativo de red 41

2.1.4 Clasificación de sistemas Operativos 43

2.1.4.1 Sistemas Operativos por lotes 44

2.1.4.2 Sistemas Operativos de tiempo real 45

2.1.4.3 Sistemas Operativos de multiprogramación (Sistemas Operativos de multitarea) 47

2.1.4.4 Sistemas Operativos de tiempo compartido 49

2.1.4.5 Sistemas Operativos distribuidos 51

2.1.4.6 Sistemas Operativos de red 52

2.1.4.7 Sistemas Operativos paralelos 53

2.2 EVALUACIÓN DE LOS SISTEMAS OPERATIVOS DE RED 53

2.2.1 Administración de recursos. 53

2.2.1.1 Compartir información (o datos) 55
2.2.1.2 Compartir hardware y software 55
2.2.1.3 Centralización de la administración y el soporte 56
2.2.2 Requisitos de Seguridad. *56*
2.2.3 Seguridad e integridad de datos. *57*
2.2.4 Desarrollo de Una Política de Seguridad. *61*
2.2.4.1 Elementos de Seguridad en Redes. 64
2.2.5 Análisis y comparación de sistemas operativos de red. *69*
2.2.5.1 Sistema operativo Unix 69
2.2.5.2 Sistema Operativo Windows NT 73
2.2.5.3 Sistema Operativo Netware de Novell 75
2.3 ATAQUES GENÉRICOS A SISTEMAS OPERATIVOS 78
2.3.1 Asincronismo: *79*
2.3.2 Rastreo: *79*
2.3.3 Entre líneas: *79*
2.3.4 Código clandestino: *79*
2.3.5 Prohibición de acceso: *80*
2.3.6 Procesos sincronizados interactivos: *80*
2.3.7 Desconexión de línea: *80*
2.3.8 Disfraz: *80*
2.3.9 Ataque "nak": *81*
2.3.10 Engaño al operador: *81*

2.3.11 Parásito: *81*

2.3.12 Caballo de Troya: *82*

2.3.13 Parámetros inesperados: *82*

3. EVALUACIÓN DE SOLUCIONES Y PLATAFORMAS DE ANTIVIRUS Y SPAMING **83**

3.1 CLASIFICACIÓN DE SOLUCIONES ANTIVIRUS Y SPAM 84

3.2 SOLUCIONES BASADAS EN ANTIVIRUS DE ESCRITORIO 85

3.2.1 Diagrama de solución basado en antivirus de Estaciones trabajo *85*

3.3 SOLUCIONES BASADAS EN SERVIDOR DE CORREO ELECTRÓNICO 86

3.3.1 Diagrama de solución basada en Servidor de correo electrónico *87*

3.4 SOLUCIONES BASADAS EN GATEWAY DE CORREO ELECTRÓNICO 88

3.4.1 Diagrama de solución basada en Gateway de correo electrónico *89*

3.4.2 VENTAJAS ADICIONALES *90*

3.4.3 DESVENTAJAS *90*

3.5 EVALUACIÓN DE SOFTWARE ANTIVIRUS 91

3.5.1 GFI MailSecurity for Exchange / SMTP *92*

3.5.1.1 Características Principales 93

3.5.1.2 Requerimientos Técnicos 99

3.5.1.3 Precios 99

3.5.2 SYMANTEC MAIL SECURITY PARA SMTP *101*

3.5.2.1 Características Principales 102

3.5.2.2 Requerimientos Técnicos 104

3.5.3 Panda SendmailSecure Antivirus *105*

3.5.3.1 Características Principales 105

3.5.3.2 Requerimientos técnicos 107

3.5.3.3 Precios 108

3.6 EVALUACIÓN DE SOFTWARE ANTISPAM 108

3.6.1 GFI MailEssentials For Exchange / SMTP *109*

3.6.1.1 Características principales 110

3.6.1.2 Requerimientos Técnicos 116

3.6.1.3 Precios 117

3.6.2 Symantec AntiSpam™ para SMTP *118*

3.6.2.1 Características principales 118

3.6.2.2 Requerimientos técnicos 123

3.6.3 Spam Assassin *124*

3.6.3.1 Características principales 125

3.7 SOLUCIONES GATEWAY APPLIANCES 127

3.7.1 PANDA GATEDEFENDER *128*

3.7.1.1 CARACTERÍSTICAS PRINCIPALES 129

3.7.1.2 REQUERIMIENTOS TECNICOS 130

3.7.2 Webshield 3000 Series Appliances *130*

3.7.2.1 CARACTERÍSTICAS PRINCIPALES 131

3.7.2.2 REQUERIMIENTOS TÉCNICOS 131

4. SELECCIÓN DE LA MEJOR SOLUCION INFORMATICA EN BASE A COSTOS, RECURSOS DE HARDWARE Y EFECTIVIDAD. 132

4.1 VENTAJAS 132

4.2 DESVENTAJAS 134

5. DISEÑO E IMPLEMENTACIÓN DE EN UN MAIL GATEWAY ENTRE UN SERVIDOR DE CORREO BASADO EN TECNOLOGIA NOVELL GROUPWISE Y UN SERVIDOR BASADO EN LINUX SEDMAIL 135

5.1.1 Especificaciones Técnicas 135

5.1.2 Diagrama de Red 137

CONCLUSIÓN Y RECOMENDACIONES 138

ANEXO - A 140

ANEXO - B 143

BIBLIOGRAFIA 144

1. VULNERABILIDADES DE LOS SERVICIOS DE CORREO ELECTRÓNICO

1.1 EL CORREO ELECTRÓNICO

1.1.1 DEFINICIÓN

El Correo Electrónico, también llamado e-mail (Electronic Mail), es una forma de enviar correo, mensajes o cartas electrónicas de un ordenador a otro a través de una red de computadoras.

1.1.2 HISTORIA DEL CORREO ELECTRÓNICO

En 1971, Ray Tomlinson inventa un programa de e-mail para mandar mensajes a través de una red distribuida y manda el primer e-mail, que era un mensaje que decía " Testing 1-2-3" y que iba dirigido a él mismo.

El segundo mensaje de e-mail, fue mucho más importante, se dirigió a todos los usuarios de ARPANET y consistió en las instrucciones y convenciones de recién inventado correo electrónico.

En 1972, Ray Tomlinson modifica el programa de correo, elige el signo @ para denotar "en" y su sistema resulta muy popular.

En 1973, un estudio de ARPA muestra que 75% del tráfico de ARPANET es correo electrónico.

John Vittal desarrolla MSG, el primer programa de correo electrónico realmente completo que incluye la posibilidad de contestar, reenviar y guardar mensajes.

En 1976, La Reina Elizabeth II de Inglaterra manda un e-mail por primera vez.

En 1977, Larry Landweber de la universidad de Wisconsin, crea THEORYNET para ofrecer correo a más de 100 investigadores en computación.

En 1979, Kevin MacKenzie manda un Email a el MsgGroup con la sugerencia de agregar una cierta emoción dentro del medio "seco" del texto del e-mail, por ejemplo: -) para indicar una sonrisa, los "emoticons" fueron y siguen siendo extensamente usados.

En 1989, se dan los primeros intercambios entre el primer proveedor comercial de correo electrónico y el Internet: MCI Mail.

[Texto tomado de : http://www.soho.com.mx/content/36e4eec7-4ad4-41ea-9076-a0606d3a3f71]

1.1.3 VENTAJAS QUE OFRECE EL CORREO ELECTRÓNICO

En realidad el e-mail es muy parecido al correo tradicional, aunque tiene varias diferencias que le proporcionan una serie de ventajas muy importantes:

Para enviar el correo tradicional, es necesario pagar por cada mensaje que se envía (sellos, sobres, papel, etc.). Sin embargo con el e-mail solo hay que disponer de una cuenta en una máquina (en ocasiones habrá que pagar si la máquina en la que se tiene la cuenta es privada, y en otras ocasiones el servicio es gratuito) y no hay los gastos antes mencionados.

El e-mail es mucho más rápido que el correo tradicional. Cuando se envía correo electrónico, puede ser cuestión de minutos que llegue a su destino, sea cual sea el lugar del mundo donde se encuentre el destinatario del mensaje. El mensaje electrónico pasa de una maquina a otra. Cada maquina que recibe un mensaje, comprueba la dirección y lo envía por la ruta correcta a otra maquina. Este proceso se repite hasta que el mensaje llega a la maquina destino, entonces se almacena en el buzón electrónico correspondiente (espacio de disco destinado a almacenar el correo electrónico de un usuario de dicha máquina). Sin embargo con el correo tradicional suele ser cuestión de días, semanas e incluso meses.

Una misma copia de un mensaje o una carta electrónica, es muy fácil distribuirla a varios destinatarios simultáneamente, con solo indicar las direcciones de estos. Con el correo tradicional esto es mas complicado, hay que hacer varias copias de la carta y pagar por cada una de ellas que se desee enviar.

Otra de las ventajas del e-mail, es que es ecológico. Cuando se usa el correo tradicional, se necesita papel, en ocasiones mucho. Con el correo electrónico, no hay papel, es un documento electrónico, que en caso de querer almacenarlo, se guarda en un fichero, con el consiguiente ahorro de papel y en definitiva de árboles, bosques, La Tierra.

Al principio, el correo electrónico, solo podía enviar mensajes de texto con mayor o menor rapidez entre usuarios. En la actualidad es posible enviar todo tipo de datos binarios gracias a estándares como MIME o UUDECODE. Se pueden incluir como parte del mensaje imágenes, sonidos, ficheros binarios, programas ejecutables, etc. Para ello es necesario que tanto el usuario que envía el correo como el que lo recibe, dispongan de un gestor de correo que cumplan o incluyan estos estándares.

Otra característica importante del e-mail, es que si un usuario tiene un acceso limitado a Internet, con su cuenta de correo puede sacar mucho provecho a servicios como el FTP, ARCHIE, LISTAS DE CORREO, etc.

Otra de las ventajas del e-mail, es que no nos tenemos que preocupar de comprobar si llegó algún tipo de correo. La maquina de la que somos usuarios, se encarga de comprobarlo por nosotros y avisarnos cuando nos conectamos a dicha máquina. En el correo tradicional, somos nosotros quienes nos encargamos de mirar en el buzón para comprobar si ha llegado algo.

Otras características del e-mail que añaden más funcionalidad son:

Es posible definir alias. Consiste en asociar un nombre, normalmente corto, a una dirección de correo electrónico. Normalmente se suelen definir alias cuando estas direcciones son utilizadas con mucha frecuencia.

Es posible organizar el correo en carpetas. Si el volumen de correo recibido es grande, será necesario almacenar ese correo por temas, por usuarios, etc. Seria algo parecido a almacenar ficheros en directorios.

Es posible la retransmisión de mensajes que nos llegan hacia otras direcciones de correo.

Lo normal en los sistemas actuales de correo, es la posibilidad de dar replica a un mensaje que nos ha llegado. Consiste en responder a un mensaje basándonos en el que nos ha llegado, tomando datos de este.

Hay muchas mas características que dan mayor funcionalidad a un sistema de correo electrónico, pero estas son las más habituales. Además dichas posibilidades dependen del software de correo electrónico usado en cada caso.

[Texto tomado de : http://usuarios.lycos.es/nachos/2.html]

1.2 ESTRUCTURA DE UN MENSAJE DE CORREO ELECTRÓNICO

En lo que se refiere a la estructura de un mensaje de correo electrónico o e-mail, es muy parecida a la estructura de una carta normal del correo tradicional. Diferenciamos dos partes fundamentales, la cabecera y el cuerpo del mensaje:

- La Cabecera actúa como de matasellos electrónico, de tal forma que cuando un usuario recibe un mensaje, puede saber a través de la información de la cabecera, quien le envió el mensaje, como fue enviado y cuando. Los campos que contiene la cabecera son:
- Nombre y dirección del usuario que envía el mensaje (FROM).
- Nombre y dirección del usuario que recibirá el mensaje (TO).
- Nombre y dirección de las copias del mensaje(CC).
- Fecha (y hora en ocasiones) del mensaje.
- Tema o asunto del mensaje (SUBJECT).

El Cuerpo del mensaje es la parte correspondiente al contenido del mensaje, que puede ser texto y en ocasiones ficheros asociados.

Hoy en día casi todos los programas de correo electrónico, permiten la incorporación de un fichero de texto que se le denominó firma. El contenido de esta firma suele ser información adicional, una frase ingeniosa, un lema, una idea, otras direcciones de correo que se disponga, incluso algún dibujo realizado con caracteres de texto.

Un aspecto importante a tener en cuenta cuando se escribe un mensaje es el de no enviar información confidencial si antes no se ha encriptado adecuadamente. Si bien es cierto que el correo electrónico en principio es privado, en realidad no lo es. Además hay muchos desaprensivos que son capaces de capturar el mensaje y usarlo para fines no adecuados.

1.3 DIRECCIONES DE CORREO ELECTRÓNICO

La dirección de correo electrónico es la forma que tenemos de especificar al programa de correo electrónico, el lugar o persona a la que queremos enviar el mensaje electrónico en concreto.

La dirección de correo electrónico tiene la siguiente estructura:

usuario @maquina.dominio

La primera parte se compone por el usuario, que nos indica el buzón de correo electrónico correspondiente a la persona a la que va destinado el mensaje, seguido de este va el símbolo arroba y a continuación se pone el nombre de la maquina o nombre del servidor donde está alojada la cuenta del usuario y por ultimo se pone un punto seguido del tipo de dominio al que pertenece la maquina. Todo lo que va después de la arroba se le suele llamar nombre completo del dominio del ordenador.

Hay varios tipos de dominios en Internet. Normalmente suelen tener como máximo 3 letras que los identifican. A continuación explico algunos:

.com: para un negocio o una empresa internacional

.edu: para una Universidad o centro de educación

.org: para una organización no comercial

.gov: para una agencia u oficina gubernamental

.mil: para una institución militar

.net: para una red determinada

En otras ocasiones se pone un indicativo del país donde esta situado el servidor geográficamente hablando:

ec: Ecuador

uk: Reino Unido

[Texto tomado de : http://usuarios.lycos.es/nachos/3.htm]

1.4 ARCHIVOS ASOCIADOS A LOS MENSAJES ELECTRÓNICOS

Hasta hace poco tiempo, con el correo electrónico solo se podían enviar mensajes de texto cortos. Para enviar o recibir ficheros, se utilizaba el servicio FTP. Hoy en día, gracias a la aparición del protocolo de Internet MIME (Multipurpose Internet Mail Extension, Extensión del correo Internet para todo propósito) y algún otro tipo de codificación como el UUDECODE, es posible enviar todo tipo de ficheros asociados a los mensajes de correo electrónico, imágenes, sonido, vídeo, ficheros binarios, ficheros ejecutables, etc.

Estos protocolos o programas se encargan de codificar los ficheros asociados y los transforman en texto ASCII, cuando se envían y el proceso contrario, cuando se reciben. Este proceso se llama "codificación" y "decodificación".

Por norma general el proceso de codificación y decodificación de los ficheros asociados se realiza de forma transparente para el usuario. El programa de correo electrónico detectará los ficheros asociados y preguntara al usuario donde desea almacenarlos en el disco duro.

[Texto tomado de : http://usuarios.lycos.es/nachos/4.htm]

1.5 PROTOCOLOS DE CORREO ELECTRÓNICO

1.5.1 HISTORIA DE LOS PROTOCOLOS DE CORREO

El correo electrónico de Internet se implementó originalmente como una función del protocolo FTP. En 1980 dos personajes, Suzanne Sluizer y Jon Postel realizaron trabajos con un protocolo que se daría en llamar posteriormente SMTP (Simple Mail Transfer Protocol). Hoy en día se sigue utilizando este protocolo para la entrega de mensajes entre sistemas de Internet.

El protocolo SMTP fue desarrollado pensando en que los sistemas que intercambiarían mensajes, eran grandes computadores, de tiempo compartido y multiusuario que estaban continuamente conectados a la red Internet. Sin embargo con la aparición de los PCs en el mundo de Internet, que tenían una conectividad ocasional, se hizo necesaria una solución para que el correo llegase a estos PCs.

Para solventar esta limitación, en 1984 surgió el POP (Post Office Protocol). Este protocolo, en su especificación inicial, solo permitía funciones básicas como recuperar todos los mensajes, mantenerlos en el servidor y borrarlos. En sucesivas versiones del protocolo (POP2, la actual versión POP3) se han ampliado las funciones que permiten una mejor gestión del correo.

Estos dos protocolos son los encargados de transportar el correo por toda la red Internet, pero solo son capaces de transportar mensajes en formato texto ASCII. Para superar esta

limitación, se utilizaba hasta hace poco tiempo, programas como el UUEncode y el UUDecode.

En 1992, surgen las MIME (Multipurpose Internet Mail Extensions), que permiten el correo electrónico en otras lenguas además del ingles, además de sonido, gráficos, vídeo, etc. En la actualidad el estándar MIME es el que se usa.

Hoy en día, el correo electrónico es entregado usando una arquitectura cliente/servidor. Un mensaje de correo electrónico es creado usando un programa de correo cliente. Este programa luego envía el mensaje a un servidor. El servidor luego lo redirige al recipiente de correo del servidor, donde el mensaje es luego suministrado al recipiente de correo del cliente.

Para habilitar todo este proceso, una variedad de protocolos de red estándar permiten que diferentes máquinas, a menudo ejecutando sistemas operativos diferentes y usando diferentes programas de correo, envíen y reciban correo electrónico o e-mail.
Los protocolos que se indican a continuación son los que más se utilizan para transferir correo electrónico de un sistema a otro.

[Texto tomado de :http://usuarios.lycos.es/nachos/7.htm]

1.6 CLASIFICACIÓN DE PROTOCOLOS DE CORREO

1.6.1 PROTOCOLOS DE TRANSPORTE DE CORREO

La entrega de correo desde una aplicación cliente a un servidor, y desde un servidor origen al servidor destino es manejada por el Protocolo (SMTP) .

1.6.1.1 EL PROTOCOLO SMTP

El significado de las siglas de SMTP es Protocolo Simple de Transmisión de Correo (Simple Mail Transfer Protocol). Este protocolo esta descrito en la RFC 821 y es el estándar de Internet para el intercambio de correo electrónico. SMTP es un protocolo independiente del subsistema de transmisión usado. Necesita que el subsistema de transmisión ponga a su disposición un canal de transmisión fiable y con entrega ordenada, con lo cual el uso del protocolo TCP en la capa de transporte es lo adecuado.

Para que dos sistemas intercambien correo mediante el protocolo SMTP, no es necesario que exista una conexión que interactué, ya que este protocolo usa métodos de almacenamiento y reenvío de mensajes.

El objetivo principal del Protocolo simple de transferencia de correo, SMTP, es transferir correo entre servidores de correo. Sin embargo es crítico para los clientes de correo también. Para poder enviar correo, el cliente envía el mensaje a un servidor de correo saliente, el cual luego contacta al servidor de correo de destino para la entrega.

Por esta razón, es necesario especificar un servidor SMTP cuando se esté configurando un cliente de correo.

Un punto importante sobre el protocolo SMTP es que no requiere autenticación. Esto permite que cualquiera en la Internet puede enviar correo a cualquiera otra personal o a grandes grupos de personal. Esta característica de SMTP es lo que hace posible el correo basura o spam. Los servidores SMTP modernos intentan minimizar este comportamiento permitiendo que sólo los hosts conocidos accedan al servidor SMTP. Los servidores que no ponen tales restricciones son llamados servidores open relay.

1.6.1.2 MODELO DE COMUNICACIONES SMTP

Cuando un sistema servidor de SMTP, desea enviar uno o varios mensajes a otro servidor SMTP, el sistema emisor establece una conexión con el sistema receptor. Esta conexión es unidireccional, es decir, que el sistema emisor puede enviar correo al receptor, pero durante esa conexión el sistema receptor no puede enviar correo al sistema emisor. Si el sistema receptor tiene que enviar correo al sistema emisor, tiene que esperar a que finalice la conexión establecida y establecer otra en sentido contrario cambiando lo papeles de emisor y receptor.

Una vez establecida la conexión, el sistema emisor envía comandos y mensajes. Los mensajes pueden tener como destino el sistema receptor o solo utilizarlo de

intermediario para llegar a un destino más lejano. El sistema receptor puede enviar al sistema emisor respuestas y códigos de estado. Los comandos son cadenas de caracteres que se pueden entender fácilmente y las respuestas son códigos numéricos seguidos de una explicación del código, que también son legibles.

Si el sistema receptor ha recibido mensajes cuyo destino es otro, entonces establece una nueva conexión con un tercer servidor SMTP y así sucesivamente hasta que los mensajes lleguen a su destino. Si el sistema receptor tiene mensajes destinados a él, entonces los distribuye entre los distintos buzones de su sistema.

[Texto tomado de :http://usuarios.lycos.es/nachos/8.htm]

1.6.2 PROTOCOLOS DE ACCESO A CORREO

Hay dos protocolos principales usados por las aplicaciones de correo cliente para recuperar correo desde los servidores de correo: el Post Office Protocol (POP) y el Internet Message Access Protocol (IMAP).

A diferencia de SMTP, estos protocolos requieren autenticación de los clientes usando un nombre de usuario y una contraseña. Por defecto, las contraseñas para ambos protocolos son pasadas a través de la red de forma encriptada.

1.6.2.1 PROTOCOLO POP

El significado de las siglas POP es Protocolo de Oficina de Correos (Post Office Protocol). El protocolo visto con anterioridad, el SMTP, se creo en un momento en el que la red Internet no estaba todavía en auge. El protocolo SMTP se creo cuando los usuarios tenían cuentas en ordenadores que estaban continuamente conectados a Internet, de tal forma que cuando un usuario quería leer su correo, entraba en una sesión de terminal y solicitaba al servidor que le diese el correo que tenia almacenado para el. Claro esta, esta situación ha cambiado considerablemente, hoy en día, los usuarios se conectan a la maquina servidora de correo por un periodo de tiempo muy breve, el suficiente para solicitar el envío del correo mediante un programa cliente. Por tanto el servidor de correo electrónico debe mantener almacenado el correo en sus buzones y enviarlo a los clientes de correo cuando estos se conecten y lo soliciten. Este es el objetivo para el cual se creo el protocolo Post Office Protocol, POP.

La situación actual es que se utiliza el protocolo SMTP para el envío de correo y para la recepción de correo se utiliza el protocolo POP, pero ya en su tercera versión desde su aparición, el POP3.

1.6.2.2 MODELO DE COMUNICACIONES POP

La descripción del protocolo POP y su modelo de comunicaciones, esta en el documento oficial estándar RFC 1725. Este modelo de comunicaciones se basa en el

concepto de buzón. Al igual que ocurre en una oficina de correos local, de una ciudad, tiene un espacio para almacenar el correo, las cartas, hasta que se recojan. De igual manera el servidor POP almacena el correo electrónico en buzones hasta que un programa cliente lo recupera.

El cliente POP se conecta con el servidor a través del puerto TCP 110. Para entrar en el servidor, es necesario una cuenta de identificación en dicha maquina (lo que le permite tener un espacio reservado para su correo). A continuación es necesario verificar que se es dueño de la cuenta a través de una clave. Una vez que se ha entrado en el sistema, el cliente POP puede dialogar con el servidor para conocer si tiene correo, cuantos mensajes tiene, que se los envíe, que los borre, etc.

Para poder ofrecer estas funciones, el modelo de comunicación POP se basa en estados. Los cuales son: estado de autorización, estado de transacción y estado de actualización. Después de establecer la conexión, el servidor POP se encuentra en un estado de autentificación o autorización, esperando a que el cliente le envíe el nombre y clave de la cuenta de usuario. Cuando se verifica que el nombre y la clave son correctos, el servidor pasa a un estado de transacción. Antes de pasar a este estado, el servidor POP hace un bloqueo del buzón para impedir que los usuarios modifique o borren el correo antes de pasar al estado siguiente. En este estado el servidor atiende a las peticiones del cliente. Después de enviar al servidor el comando QUIT el servidor pasa al estado de

actualización, en este estado el servidor elimina los mensajes que estaban con la marca de borrado y finaliza la conexión.

[Texto tomado de :http://usuarios.lycos.es/nachos/9.htm]

1.6.2.3 IMAP

Cuando utilice un servidor de correo IMAP, los mensajes de correo se mantienen en el servidor donde los usuarios pueden leer y borrarlos. IMAP también permite a las aplicaciones cliente crear, renombrar o borrar directorios en el servidor para organizar y almacenar correo.

IMAP lo utilizan principalmente los usuarios que accedan su correo desde varias máquinas. El protocolo es conveniente también para usuarios que se estén conectando al servidor de correo a través de una conexión lenta, porque sólo la información de la cabecera del correo es descargada para los mensajes, hasta que son abiertos, ahorrando de esta forma ancho de banda. El usuario también tiene la habilidad de eliminar mensajes sin verlos o descargarlos.

Por conveniencia, las aplicaciones cliente IMAP son capaces de hacer caché de los mensajes localmente, para que el usuario pueda hojear los mensajes previamente leídos cuando no se esté conectado directamente al servidor IMAP.

IMAP, como POP, es completamente compatible con estándares de mensajería de Internet, tales como MIME, que permite los anexos de correo.

También están disponibles otros clientes y servidores de correo IMAP gratuitos así como también comerciales, muchos de los cuales extienden el protocolo IMAP y proporcionan funcionalidades adicionales.

[Texto tomado de : http://www.europe.redhat.com/documentation/rhl9/rhl-rg-es-9/ch-email.php3]

1.7 CLASIFICACIONES DE LOS PROGRAMAS DE CORREO

En general, todas las aplicaciones de e-mail caen en al menos una de tres clasificaciones. Cada clasificación juega un papel específico en el proceso de mover y administrar los mensajes de correo. Mientras que la mayoría de los usuarios sólo están al tanto del programa de correo específico que usan para recibir o enviar mensajes, cada uno es importante para asegurar que el mensaje llegue a su destino correcto.

1.7.1 AGENTE DE TRANSFERENCIA DE CORREO

Un Agente de transferencia de correo (MTA) transfiere mensajes de correo electrónico entre hosts usando SMTP. Un mensaje puede envolver a muchos MTAs a medida que este se mueve hasta llegar a su destino.

Aunque la entrega de mensajes entre máquinas puede parecer bien simple, el proceso completo de decidir si un MTA particular puede o debería aceptar un mensaje para ser repartido, es más bien complicada. Además, debido a los problemas de Spam, el uso de un MTA particular está usualmente restringido por la configuración del MTA o por la falta de acceso a la red MTA.

Muchos programas clientes de correo modernos pueden actuar como un MTA cuando estén enviando correo. Sin embargo, esta acción no debería ser confundida con el papel de un MTA verdadero. La única razón de que los programas de correo cliente son capaces de enviar mensajes (como un MTA) es porque el host ejecutando la aplicación no tiene su propio MTA.. Sin embargo, estos programas clientes sólo envían mensajes hacia fuera, hacia un MTA para el cual están autorizados a utilizar y no directamente al servidor de correos recipiente.

1.7.2 AGENTE DE ENTREGA DE CORREO

Un Agente de entrega de correos (MDA) es invocado por un MTA para archivar correo entrante en el buzón de correo del usuario. En muchos casos, el MDA es en realidad un Agente de entregas local (LDA).

Cualquier programa que realmente maneja un mensaje para entrega al punto en que puede ser leído por una aplicación cliente de correos se puede considerar un MDA. Por esta razón, algunos MTAs pueden tener el papel de un MDA cuando ellos anexan nuevos mensajes de correo al archivo spool de correo del usuario. En general, los MDAs no transportan mensajes entre sistemas tampoco proporcionan una interfaz de usuario; los MDAs distribuyen y clasifican mensajes en la máquina local para que lo accese una aplicación cliente de correo.

1.7.3 AGENTE DE USUARIO DE CORREO

Un *agente de usuario de correo* (*MUA*) es sinónimo con una aplicación cliente de correo. Un MUA es un programa que, al menos, le permite a los usuarios leer y redactar mensajes de correo. Muchos MUAs son capaces de recuperar mensajes a través de los protocolos POP o IMAP, configurando los buzones de correo para almacenar mensajes y enviando los mensajes salientes a un MTA.

1.7.4 ARQUITECTURA Y SERVICIOS

Los sistemas de correo electrónico se integran básicamente de dos subsistemas:

- El agente usuario (MUA), que coloca los mensajes en la cola del correo electrónico.
- El agente de transferencia de mensajes (MTA), que es el responsable de inicializar el enlace de comunicación con las computadoras remotas y transmitir el correo electrónico.

La aplicación del agente usuario son los programas locales que ofrecen una interacción con el sistema de correo electrónico sobre la base de línea de comando, basados en menús o con una interfase gráfica. Los agentes transferencia de mensajes son usualmente los procesos del sistema operativo, y mueven el correo electrónico a través del sistema o de la red. Un sistema de correo electrónico soporta cinco funciones básicas: composición, transferencia, reporte, despliegue y disposición.

Además, a estos servicios básicos, la mayoría de los sistemas de correo electrónico ofrecen una amplia variedad de características avanzadas para administrar los mensajes del usuario. Un servicio muy usado en el correo electrónico son las listas de interés, las cuales permiten con sólo enviar un mensaje a la lista de correo electrónico en particular, repartir una copia idéntica del mensaje a todos los subscriptores de la lista, lo que evita la necesidad de enviar un correo electrónico a cada uno de ellos.

Una idea clave en todos los sistemas modernos de correo electrónico es la distinción entre el sobre y su contenido. El sobre envuelve el mensaje. Este contiene toda la información necesaria para transportar el mensaje, tales como la dirección destino, prioridad y nivel de seguridad, lo anterior es distinta del mensaje por sí mismo. El agente transporte usa el sobre para el enrutamiento del mensaje.

[Texto tomado de: http://www.europe.redhat.com/documentation/rhl9/rhl-rg-es-9/s1-email-types.php3]

1.8 VULNERABILIDADES DE CORREO ELECTRÓNICO

1.8.1 ¿QUÉ ES UNA VULNERABILIDAD?

Una vulnerabilidad utiliza debilidades conocidas en aplicaciones o sistemas operativos para comprometer la seguridad de un sistema, por ejemplo ejecutar un programa o comando, o instalar una `puerta trasera'.

Estas debilidades permiten que se explote o abuse de una característica particular en un programa o del sistema operativo para su propio uso. Algunos programas poseen "agujeros" que pueden facilitar la infección de nuestro ordenador.

Como en el mito griego del famoso héroe Aquiles, una vulnerabilidad representa un punto a través del cual es posible vencer la seguridad de un ordenador. Una vulnerabilidad es un fallo en la programación de una aplicación cualquiera, y que puede ser aprovechado para llevar a cabo una intrusión en el ordenador que tenga instalado dicho programa.

Generalmente, dicho fallo de programación se refiere a operaciones que provocan un funcionamiento anormal de la aplicación. Esta situación anómala puede ser producida artificialmente por una persona maliciosa para poder introducirse en un ordenador sin el consentimiento del usuario. En ocasiones, es suficiente con abrir un documento creado "artesanalmente" con ese fin específico.

Esto le permitirá al usuario malicioso realizar un gran abanico de acciones en el ordenador vulnerable, desde ejecutar ficheros hasta borrarlos, introducir virus, acceder a información, etc.

Aunque son más conocidas las vulnerabilidades asociadas a sistemas operativos, navegadores de Internet y programas de correo electrónico, cualquier programa puede presentar vulnerabilidades: procesadores de textos, bases de datos, aplicaciones de reproducción de archivos de sonido, etc.

Una vulnerabilidad no representa un peligro inmediato para el ordenador. Sin embargo, es una vía de entrada potencial para otras amenazas, tales como virus, gusanos, troyanos y puertas traseras, que sí pueden tener efectos destructivos.

Por ello, es altamente recomendable estar informado acerca de las vulnerabilidades descubiertas en los programas instalados y aplicar los parches de seguridad más recientes proporcionados por la empresa fabricante, accesibles a través del sitio web de la misma.

[Texto tomado de : http://usuarios.lycos.es/accimt/apuntes/si3.html]

1.8.2 ¿QUÉ ES UNA VULNERABILIDAD DE CORREO?

Una vulnerabilidad de correo es un exploit lanzado mediante correo electrónico. Un `exploit' de correo es esencialmente una debilidad que puede estar incrustada en un correo, y ser ejecutado sobre el equipo del destinatario una vez abra o reciba el correo. Esto permite al hacker eludir los cortafuegos y productos antivirus.

1.8.3 VULNERABILIDADES DE CORREO ELECTRÓNICO POR CONTENIDO HTML

Mediante el uso de scripts en el código HTML, intrusos pueden leer el correo electrónico de terceros, enviar correo usurpando identidades e incluso hacerse del

control de un PC intervenido.

[Texto tomado de : http://support.gfi.com/manuals/es/msec8/msec8manual_es-1-39.html]

1.8.4 AMENAZAS DE LOS SISTEMAS DE CORREO

Existen muchas amenazas a las están expuestos los sistemas de mensajería electrónica en los actuales momentos.

Los virus informáticos junto con los caballos de Troya, los programas espías y el spam se han convertido en las principales amenazas y las detallaremos a continuación.

1.8.5 ¿QUÉ ES UN VIRUS?

Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta "entidades ejecutables": cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar.

1.8.6 PRINCIPALES CARACTERÍSTICAS DE UN VIRUS INFORMÁTICO

Es dañino. Un virus informático siempre causa daños en el sistema que infecta. El virus busca destruir o alterar información o provocar efectos negativos para la computadora, como consumo de memoria principal, tiempo de procesador, disminución de la performance.

Es auto reproductor. La característica más importante de este tipo de programas es la de crear copias de sí mismo, cosa que ningún otro programa convencional hace.

Es subrepticio. Utiliza varias técnicas para evitar ser detectado y que el usuario no se de cuenta de su presencia..

1.8.7 CLASIFICACIÓN DE LOS VIRUS

La clasificación de los virus siempre resulta variada según sea la manera en que los podamos agrupar: Estas pueden ser por la entidad que parásita (sectores de arranque o archivos ejecutables), por su grado de dispersión a nivel mundial, por su comportamiento, por su agresividad, por sus técnicas de ataque o por como se oculta.

Nuestra clasificación muestra como actúa cada uno de los diferentes tipos según su comportamiento. En algunos casos un virus puede incluirse en más de un tipo

1.8.7.1 CABALLOS DE TROYA

Los caballos de Troya no llegan a ser realmente virus porque no tienen la capacidad de auto reproducirse. Se esconden dentro del código de archivos ejecutables y no ejecutables pasando inadvertidos por los controles de muchos antivirus. Posee subrutinas que permitirán que se ejecute en el momento oportuno. Existen diferentes caballos de Troya que se centrarán en distintos puntos de ataque. Su objetivo será el de robar las contraseñas que el usuario tenga en sus archivos o las contraseñas para el acceso a redes, incluyendo a Internet. Después de que el virus obtenga la contraseña que deseaba, la enviará por correo electrónico a la dirección que tenga registrada como la de la persona que lo envió a realizar esa tarea.

Un caballo de Troya que infecta la red de una empresa representa un gran riesgo para la seguridad, ya que está facilitando enormemente el acceso de los intrusos. Muchos caballos de Troya utilizados para espionaje industrial están programados para autodestruirse una vez que cumplan el objetivo para el que fueron programados, destruyendo toda la evidencia.

1.8.7.2 CAMALEONES

Son una variedad de similar a los Caballos de Troya, pero actúan como otros programas comerciales, en los que el usuario confía, mientras que en realidad están haciendo algún

tipo de daño. Cuando están correctamente programados, los camaleones pueden realizar todas las funciones de los programas legítimos a los que sustituyen (actúan como programas de demostración de productos, los cuales son simulaciones de programas reales).

1.8.7.3 VIRUS POLIMORFOS O MUTANTES

Los virus polimorfos poseen la capacidad de encriptar el cuerpo del virus para que no pueda ser detectado fácilmente por un antivirus. Solo deja disponibles unas cuantas rutinas que se encargaran de desencriptar el virus para poder propagarse. Una vez desencriptado el virus intentará alojarse en algún archivo de la computadora.

En este punto tenemos un virus que presenta otra forma distinta a la primera, su modo desencriptado, en el que puede infectar y hacer de las suyas libremente. Pero para que el virus presente su característica de cambio de formas debe poseer algunas rutinas especiales. Si mantuviera siempre su estructura, esté encriptado o no, cualquier antivirus podría reconocer ese patrón.

Para eso incluye un generador de códigos al que se conoce como motor de mutación. Este motor utiliza un generador numérico aleatorio que, combinado con un algoritmo matemático, modifica la firma del virus. Gracias a este motor de mutación el virus podrá crear una rutina de desencriptar que será diferente cada vez que se ejecute.

1.8.7.4 VIRUS SIGILOSO O STEALTH

El virus sigiloso posee un módulo de defensa bastante sofisticado. Este intentará permanecer oculto tapando todas las modificaciones que haga y observando cómo el sistema operativo trabaja con los archivos y con el sector de arranque. Subvirtiendo algunas líneas de código el virus logra apuntar el flujo de ejecución hacia donde se encuentra la zona que infectada.

Es difícil que un antivirus se de cuenta de estas modificaciones por lo que será imperativo que el virus se encuentre ejecutándose en memoria en el momento justo en que el antivirus corre. Los antivirus de hoy en día cuentan con la técnica de verificación de integridad para detectar los cambios realizados en las entidades ejecutables.

1.8.7.5 RETRO-VIRUS O VIRUS ANTIVIRUS

Un retro-virus intenta como método de defensa atacar directamente al programa antivirus incluido en la computadora.

Generalmente los retro-virus buscan el archivo de definición de virus y lo eliminan, imposibilitando al antivirus la identificación de sus enemigos. Suelen hacer lo mismo con el registro del comprobador de integridad.

1.8.7.6 VIRUS MULTIPARTITOS

Los virus multipartitos atacan a los sectores de arranque y a los ficheros ejecutables. Su nombre está dado porque infectan las computadoras de varias formas. No se limitan a infectar un tipo de archivo ni una zona de la unidad de disco rígido. Cuando se ejecuta una aplicación infectada con uno de estos virus, éste infecta el sector de arranque. La próxima vez que arranque la computadora, el virus atacará a cualquier programa que se ejecute.

1.8.7.7 VIRUS VORACES

Estos virus alteran el contenido de los archivos de forma indiscriminada. Generalmente uno de estos virus sustituirá el programa ejecutable por su propio código. Son muy peligrosos porque se dedican a destruir completamente los datos que puedan encontrar.

1.8.7.8 BOMBAS DE TIEMPO

Son virus convencionales y pueden tener una o más de las características de los demás tipos de virus pero la diferencia está dada por el trigger de su módulo de ataque que se disparará en una fecha determinada. No siempre pretenden crear un daño específico. Por lo general muestran mensajes en la pantalla en alguna fecha que representa un evento importante para el programador.

1.8.7.9 MACRO-VIRUS

Los macro-virus representan una de las amenazas más importantes para una red, actualmente son los virus que más se están extendiendo a través de Internet. Representan una amenaza tanto para las redes informáticas como para los ordenadores independientes. Su máximo peligro está en que son completamente independientes del sistema operativo o de la plataforma. Es más, ni siquiera son programas ejecutables.

Los macro-virus son pequeños programas escritos en el lenguaje propio (conocido como lenguaje script o macro-lenguaje) propio de un programa. Así nos podemos encontrar con macro-virus para editores de texto, hojas de cálculo y utilidades especializadas en la manipulación de imágenes.

1.8.7.10 GUSANOS

Un gusano se puede decir que es un set de programas, que tiene la capacidad de desparramar un segmento de el o su propio cuerpo a otras computadoras conectadas a una red.

Hay dos tipos de Gusanos:

Host Computer Worm

Son contenidos totalmente en una computadora, se ejecutan y se copian a si mismo vía conexión de una red. Los Host Computer Worm, originalmente terminan cuando hicieron una copia de ellos mismos en otro host. Entonces, solo hay una copia del gusano corriendo en algún lugar de una red. También existen los Host Computer Worm, que hacen una copia de ellos mismos e infectan otras redes, es decir, que cada maquina guarda una copia de este Gusano.

Network Worm

Consisten en un conjunto de partes (llamadas "segmentos"), cada una corre en una maquina distinta (y seguramente cada una realiza una tarea distinta) y usando la red para distintos propósitos de comunicación.

[Texto tomado de: http://www.monografias.com/trabajos12/virudos/virudos.shtml]

1.8.8 ¿ QUÉ ES SPAM ?

El spam es el hecho de enviar mensajes electrónicos generalmente de tipo comercial. Estos no son solicitados y se reciben en cantidades masivas. Aunque el spam se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico.

1.8.9 TÉCNICAS SPAM

Los spammers, llamados así a los individuos o empresas que envían spam, utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de robots o programas automáticos que recorren Internet en busca de direcciones. Algunas de las principales fuentes de direcciones para luego enviar el spam serán mencionadas a continuación.

1.8.9.1 OBTENCIÓN DE DIRECCIONES DE CORREO

- Las propias páginas Web, que con frecuencia contienen la dirección de su creador, o de sus visitantes (en foros, weblogs, etc.).

- Los grupos de noticias de usenet cuyos mensajes suelen incluir la dirección del remitente.

- Correos electrónicos con chistes, cadenas, etc. que los usuarios de Internet suelen reenviar sin ocultar las direcciones, y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje.

- Páginas en las que se solicita una dirección de correo para acceder a un determinado servicio o descarga.

- Compra de bases de datos de direcciones de correo a empresas o particulares que aunque es ilegal en la mayor parte de los países se da con mucha frecuencia.

- Entrada ilegal en servidores. Por ensayo y error: En éste método se generan aleatoria mente direcciones, y se comprueba luego si han llegado los mensajes. Un método habitual es hacer una lista de dominios, y agregarles "prefijos" habituales. Por ejemplo, para el dominio microsoft.com, se puede probar con info@microsoft.com, webmaster@microsoft.com, staff@microsoft.com, etc.

1.8.9.2 ENVÍO DE LOS MENSAJES

Una vez tienen una gran cantidad de direcciones de correo, los spammers utilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones. Esto supone un costo mínimo para ellos, pero perjudica al receptor generando pérdidas económicas y de tiempo. Este perjuicio afecta al Internet, por consumirse gran parte del ancho de banda en mensajes basura.

1.8.9.3 VERIFICACIÓN DE LA RECEPCIÓN

Además, es frecuente que el spammer controle qué direcciones funcionan y cuáles no por medio de Web bugs, pequeñas imágenes o similares que están contenidas en el código HTML del mensaje. De esta forma, cada vez que alguien lee el mensaje, su ordenador solicita la imagen al servidor del spammer, que registra automáticamente el hecho. Son una forma más de spyware. Otro sistema es el de prometer en los mensajes que enviando un mail a una dirección se dejará de recibirlos: cuando alguien contesta, significa no sólo que lo ha abierto, sino que lo ha leído.

1.8.9.4 TROYANOS Y ORDENADORES ZOMBIS

Esta técnica es mucho más perniciosa y que es la creación de virus troyanos que se expanden masivamente por ordenadores no protegidos o sea sin cortafuegos. De ésta manera los ordenadores infectados son utilizados por el spammer como "ordenadores zombis", que envían spam a sus órdenes, pudiendo incluso rastrear los discos duros en busca de más direcciones.

[Texto tomado de : http://enciclopedia.us.es/index.php/Correo_basura]

1.9 ALTERNATIVAS PARA CORREO ELECTRÓNICO SEGURO

Como objetivo principal de ésta tesis tenemos los sistemas de protección antivirus, el filtrado de contenidos y el control del spam para sistemas de correo electrónico. Sin

embargo para complementar este ambiente de seguridad en los sistemas de correo electrónico debemos mencionar la importancia de mantener medidas de seguridad en la privacidad e integridad y garantizar la autenticidad en el correo electrónico.

Cualquier herramienta para correo electrónico seguro ha de tener tres características:

- Debe ser surtido por varios vendedores o productores.
- Debe ser ínter operable
- Debe ser aprobado o avalado por las entidades estandarizadoras de Internet.

Entre los rasgos que debe mantener están:

- La privacidad, es decir, el encriptamiento de datos.
- La autentificación, que conlleva la integridad de los mensajes.
- El manejo de llaves publicas y privadas

En el correo electrónico, el encriptamiento se hace por lo general con métodos de llave pública y la revisión de integridad mediante firmas electrónicas y funciones de dispersión para construir compendios a la manera de sumas de prueba.

Existen herramientas como S/MIME y PGP que permiten ofrecer los servicios de seguridad que hemos mencionado

Actualmente existen diversos proveedores de servidores de correo electrónico y en estos productos se incluyen a S/MIME, PGP/MIME y OpenPGP.

[Texto tomado de : http://enciclopedia.us.es/index.php/Correo_basura]

2. EVALUACIÓN DE DIFERENTES SISTEMAS OPERATIVOS DE RED Y SU IMPACTO ANTE LOS VIRUS

2.1 SISTEMAS OPERATIVOS DE RED

2.1.1 INTRODUCCIÓN

Las computadoras han evolucionado de una manera impresionante, hoy en día son las herramientas mas empleadas por el hombre y cada día se tratan de hacer más eficientes, precisas y veloces. Esta evolución de las computadoras va de la mano con su software, que es todos aquellos programas que no podemos ver físicamente, pero si los podemos usar para redactar un texto, navegar por Internet, programar, etc.

Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red. Si no se dispone de ningún sistema operativo de red, los equipos no pueden compartir recursos y los usuarios no pueden utilizar estos recursos.

El software del sistema operativo de red se integra en un número importante de sistemas operativos conocidos, incluyendo Windows 2000 Server/Professional, Windows NT Server/Workstation, Windows 95/98/ME y Apple Talk.

Cada configuración (sistemas operativos de red y del equipo separado, o sistema operativo combinando las funciones de ambos) tiene sus ventajas e inconvenientes. Por tanto, nuestro trabajo como especialistas en redes es determinar la configuración que mejor se adapte a las necesidades de nuestra red.

El sistema operativo de un equipo coordina la interacción entre el equipo y los programas (o aplicaciones) que está ejecutando. Controla la asignación y utilización de los recursos hardware tales como:

- Memoria.
- Tiempo de CPU.
- Espacio de disco.

En un entorno de red, los servidores proporcionan recursos a los clientes de la red y el software de red del cliente permite que estos recursos estén disponibles para los equipos clientes. La red y el sistema operativo del cliente están coordinados de forma que todos los elementos de la red funcionen correctamente.

2.1.2 DEFINICIÓN DE SISTEMA OPERATIVO DE RED

Un Sistema Operativo es una parte importante de cualquier sistema de computación. Un sistema de computación puede dividirse en cuatro componentes: el hardware, el Sistema Operativo, los programas de aplicación y los usuarios. El hardware (Unidad Central de Procesamiento (UCP), memoria y dispositivos de entrada/salida (E/S)) proporciona los recursos de computación básicos. Los programas de aplicación (compiladores, sistemas de bases de datos, juegos de video y programas para negocios) definen la forma en que estos recursos se emplean para resolver los problemas de computación de los usuarios.

Los Sistemas Operativos son ante todo administradores de recursos; el principal recurso que administran es el hardware del computador; además de los procesadores, los medios de almacenamiento, los dispositivos de entrada/salida, los dispositivos de comunicación y los datos.

Un Sistema Operativo es un conjunto de programas que controla la ejecución de programas de aplicación y actúa como una interfaz entre el usuario y el hardware de una computadora, esto es, un Sistema Operativo explota y administra los recursos de hardware de la computadora con el objeto de proporcionar un conjunto de servicios a los usuarios del sistema, es decir que los Sistemas Operativos son un conjunto de programas que crean la interfaz del hardware con el usuario, y que tiene dos funciones primordiales, que son:

Gestionar el hardware.- Se refiere al hecho de administrar de una forma más eficiente los recursos de la máquina.

Facilitar el trabajo al usuario.- Permite una comunicación con los dispositivos de la máquina.

El Sistema Operativo se encuentra almacenado en la memoria secundaria. Primero se carga y ejecuta un pedazo de código que se encuentra en el procesador, el cual carga el BIOS, y este a su vez carga el Sistema Operativo que carga todos los programas de aplicación y software variado.

2.1.3 CARACTERÍSTICAS DE UN SISTEMA OPERATIVO DE RED

Un Sistema Operativo tiene las siguientes características:

- Conveniencia. Un Sistema Operativo hace más conveniente el uso de una computadora.
- Eficiencia. Un Sistema Operativo permite que los recursos de la computadora se usen de la manera más eficiente posible.
- Habilidad para evolucionar. Un Sistema Operativo deberá construirse de manera que permita el desarrollo, prueba o introducción efectiva de nuevas funciones del sistema sin interferir con el servicio.

- Encargado de administrar el hardware. El Sistema Operativo se encarga de manejar de una mejor manera los recursos de la computadora en cuanto a hardware se refiere, esto es, asignar a cada proceso una parte del procesador para poder compartir los recursos.
- Relacionar dispositivos (gestionar a través del kernel). El Sistema Operativo se debe encargar de comunicar a los dispositivos periféricos, cuando el usuario así lo requiera.
- Organizar datos para acceso rápido y seguro.
- Manejar las comunicaciones en red. El Sistema Operativo permite al usuario manejar con alta facilidad todo lo referente a la instalación y uso de las redes de computadoras.
- Procesamiento por bytes de flujo a través del bus de datos.
- Facilitar las entradas y salidas. Un Sistema Operativo debe hacerle fácil al usuario el acceso y manejo de los dispositivos de Entrada/Salida de la computadora.
- Técnicas de recuperación de errores.
- Evita que otros usuarios interfieran. El Sistema Operativo evita que los usuarios se bloqueen entre ellos, informándoles si esa aplicación esta siendo ocupada por otro usuario.
- Generación de estadísticas.
- Permite que se puedan compartir el hardware y los datos entre los usuarios.

El software de aplicación son programas que se utilizan para diseñar, tal como el procesador de palabras, lenguajes de programación, hojas de cálculo, etc.

El software de base sirve para interactuar el usuario con la máquina, son un conjunto de programas que facilitan el ambiente plataforma, y permite el diseño del mismo.
El Software de base está compuesto por :

- Cargadores.
- Compiladores.
- Ensambladores.
- Macros.

[Texto tomado de : http://www.monografias.com/trabajos/soredes/soredes.shtml]

2.1.4 CLASIFICACIÓN DE SISTEMAS OPERATIVOS

Los Sistemas Operativos fueron clasificándose de diferentes maneras a través del tiempo, dependiendo del uso o de la aplicación que se les daba. A continuación se mostrarán diversos Sistemas Operativos que existen en la actualidad, con algunas de sus características:

2.1.4.1 SISTEMAS OPERATIVOS POR LOTES

Los Sistemas Operativos por lotes, procesan una gran cantidad de trabajos con poca o ninguna interacción entre los usuarios y los programas en ejecución. Se reúnen todos los trabajos comunes para realizarlos al mismo tiempo, evitando la espera de dos o más trabajos como sucede en el procesamiento en serie. Estos sistemas son de los más tradicionales y antiguos, y fueron introducidos alrededor de 1956 para aumentar la capacidad de procesamiento de los programas.

Cuando estos sistemas son bien planeados, pueden tener un tiempo de ejecución muy alto, porque el procesador es mejor utilizado y los Sistemas Operativos pueden ser simples, debido a la secuenciabilidad de la ejecución de los trabajos.
Algunos ejemplos de Sistemas Operativos por lotes exitosos son el SCOPE, del DC6600, el cual está orientado a procesamiento científico pesado, y el EXEC II para el UNIVAC 1107, orientado a procesamiento académico.

Algunas otras características con que cuentan los Sistemas Operativos por lotes son:

- Requiere que el programa, datos y órdenes al sistema sean remitidos todos juntos en forma de lote.
- Permiten poca o ninguna interacción usuario/programa en ejecución.
- Mayor potencial de utilización de recursos que procesamiento serial simple en sistemas multiusuarios.

- No conveniente para desarrollo de programas por bajo tiempo de retorno y depuración fuera de línea.
- Conveniente para programas de largos tiempos de ejecución (Ej., análisis estadísticos, nóminas de personal, etc.).
- Se encuentra en muchos computadores personales combinados con procesamiento serial.
- Planificación del procesador sencilla, típicamente procesados en orden de llegada.
- Planificación de memoria sencilla, generalmente se divide en dos: parte residente del S.O. y programas transitorios.
- No requieren gestión crítica de dispositivos en el tiempo.
- Suelen proporcionar gestión sencilla de manejo de archivos: se requiere poca protección y ningún control de concurrencia para el acceso.

2.1.4.2 SISTEMAS OPERATIVOS DE TIEMPO REAL

Los Sistemas Operativos de tiempo real son aquellos en los cuales no tiene importancia el usuario, sino los procesos. Por lo general, están subutilizados sus recursos con la finalidad de prestar atención a los procesos en el momento que lo requieran. Se utilizan en entornos donde son procesados un gran número de sucesos o eventos.

Muchos Sistemas Operativos de tiempo real son construidos para aplicaciones muy específicas como control de tráfico aéreo, bolsas de valores, control de refinerías, control de laminadores. También en el ramo automovilístico y de la electrónica de consumo, las aplicaciones de tiempo real están creciendo muy rápidamente. Otros campos de aplicación de los Sistemas Operativos de tiempo real son los siguientes:

- Control de trenes.
- Telecomunicaciones.
- Sistemas de fabricación integrada.
- Producción y distribución de energía eléctrica.
- Control de edificios.
- Sistemas multimedia.

Algunos ejemplos de Sistemas Operativos de tiempo real son: VxWorks, Solaris, Lyns OS y Spectra. Los Sistemas Operativos de tiempo real, cuentan con las siguientes características:

- Se dan en entornos en donde deben ser aceptados y procesados gran cantidad de sucesos, la mayoría externos al sistema computacional, en breve tiempo o dentro de ciertos plazos.
- Se utilizan en control industrial, conmutación telefónica, control de vuelo, simulaciones en tiempo real., aplicaciones militares, etc.

- Objetivo es proporcionar rápidos tiempos de respuesta.
- Procesa ráfagas de miles de interrupciones por segundo sin perder un solo suceso.
- Proceso se activa tras ocurrencia de suceso, mediante interrupción.
- Proceso de mayor prioridad expropia recursos.
- Por tanto generalmente se utiliza planificación expropiativa basada en prioridades.
- Gestión de memoria menos exigente que tiempo compartido, usualmente procesos son residentes permanentes en memoria.
- Población de procesos estática en gran medida.
- Poco movimiento de programas entre almacenamiento secundario y memoria.
- Gestión de archivos se orienta más a velocidad de acceso que a utilización eficiente del recurso.

2.1.4.3 SISTEMAS OPERATIVOS DE MULTIPROGRAMACIÓN (SISTEMAS OPERATIVOS DE MULTITAREA)

Se distinguen por sus habilidades para poder soportar la ejecución de dos o más trabajos activos (que se están ejecutado) al mismo tiempo.

Esto trae como resultado que la Unidad Central de Procesamiento (UCP) siempre tenga alguna tarea que ejecutar, aprovechando al máximo su utilización.

Su objetivo es tener a varias tareas en la memoria principal, de manera que cada uno está usando el procesador, o un procesador distinto, es decir, involucra máquinas con más de una UCP.

Sistemas Operativos como UNIX, Windows 95, Windows 98, Windows NT, MAC-OS, OS/2, soportan la multitarea.

Las características de un Sistema Operativo de multiprogramación o multitarea son las siguientes:

- Mejora productividad del sistema y utilización de recursos.
- Multiplexa recursos entre varios programas.
- Generalmente soportan múltiples usuarios (multiusuarios).
- Proporcionan facilidades para mantener el entorno de usuarios individuales.
- Requieren validación de usuario para seguridad y protección.
- Proporcionan contabilidad del uso de los recursos por parte de los usuarios.

- Multitarea sin soporte multiusuario se encuentra en algunos computadores personales o en sistemas de tiempo real.
- Sistemas multiprocesadores son sistemas multitareas por definición ya que soportan la ejecución simultánea de múltiples tareas sobre diferentes procesadores.

En general, los sistemas de multiprogramación se caracterizan por tener múltiples programas activos compitiendo por los recursos del sistema: procesador, memoria, dispositivos periféricos.

2.1.4.4 SISTEMAS OPERATIVOS DE TIEMPO COMPARTIDO

Permiten la simulación de que el sistema y sus recursos son todos para cada usuario. El usuario hace una petición a la computadora, esta la procesa tan pronto como le es posible, y la respuesta aparecerá en la Terminal del usuario.

Los principales recursos del sistema, el procesador, la memoria, dispositivos de E/S, son continuamente utilizados entre los diversos usuarios, dando a cada usuario la ilusión de que tiene el sistema dedicado para sí mismo. Esto trae como consecuencia una gran carga de trabajo al Sistema Operativo, principalmente en la administración de memoria principal y secundaria.

Ejemplos de Sistemas Operativos de tiempo compartido son Multics, OS/360 y DEC-10.

Características de los Sistemas Operativos de tiempo compartido:

- Populares representantes de sistemas multiprogramados multiusuario, Ej.: sistemas de diseño asistido por computador, procesamiento de texto, etc.
- Dan la ilusión de que cada usuario tiene una máquina para sí.
- Mayoría utilizan algoritmo de reparto circular.
- Programas se ejecutan con prioridad rotatoria que se incrementa con la espera y disminuye después de concedido el servicio.
- Evitan monopolización del sistema asignando tiempos de procesador (time slot).
- Gestión de memoria proporciona protección a programas residentes.
- Gestión de archivo debe proporcionar protección y control de acceso debido a que pueden existir múltiples usuarios accesando un mismo archivo.

2.1.4.5 SISTEMAS OPERATIVOS DISTRIBUIDOS

Permiten distribuir trabajos, tareas o procesos, entre un conjunto de procesadores. Puede ser que este conjunto de procesadores esté en un equipo o en diferentes, en este caso es transparente para el usuario. Existen dos esquemas básicos de éstos. Un sistema fuertemente acoplado es a es aquel que comparte la memoria y un reloj global, cuyos tiempos de acceso son similares para todos los procesadores. En un sistema débilmente acoplado los procesadores no comparten ni memoria ni reloj, ya que cada uno cuenta con su memoria local.

Los sistemas distribuidos deben de ser muy confiables, ya que si un componente del sistema se compone otro componente debe de ser capaz de reemplazarlo.

Entre los diferentes Sistemas Operativos distribuidos que existen tenemos los siguientes: Sprite, Solaris-MC, Mach, Chorus, Spring, Amoeba, Taos, etc.

Características de los Sistemas Operativos distribuidos:

- Colección de sistemas autónomos capaces de comunicación y cooperación mediante interconexiones hardware y software.
- Gobierna operación de un S.C. y proporciona abstracción de máquina virtual a los usuarios.
- Objetivo clave es la transparencia.

- Generalmente proporcionan medios para la compartición global de recursos.
- Servicios añadidos: denominación global, sistemas de archivos distribuidos, facilidades para distribución de cálculos (a través de comunicación de procesos internodos, llamadas a procedimientos remotos, etc.).

2.1.4.6 SISTEMAS OPERATIVOS DE RED

Son aquellos sistemas que mantienen a dos o más computadoras unidas a través de algún medio de comunicación (físico o no), con el objetivo primordial de poder compartir los diferentes recursos y la información del sistema.

El primer Sistema Operativo de red estaba enfocado a equipos con un procesador Motorola 68000, pasando posteriormente a procesadores Intel como Novell Netware.

Los Sistemas Operativos de red mas ampliamente usados son: Novell Netware, Personal Netware, LAN Manager, Windows NT Server, UNIX, LANtastic.

2.1.4.7 SISTEMAS OPERATIVOS PARALELOS

En estos tipos de Sistemas Operativos se pretende que cuando existan dos o más procesos que compitan por algún recurso se puedan realizar o ejecutar al mismo tiempo.

En UNIX existe también la posibilidad de ejecutar programas sin tener que atenderlos en forma interactiva, simulando paralelismo (es decir, atender de manera concurrente varios procesos de un mismo usuario). Así, en lugar de esperar a que el proceso termine de ejecutarse (como lo haría normalmente), regresa a atender al usuario inmediatamente después de haber creado el proceso.

Ejemplos de estos tipos de Sistemas Operativos están: Alpha, PVM, la serie AIX, que es utilizado en los sistemas RS/6000 de IBM.

2.2 EVALUACIÓN DE LOS SISTEMAS OPERATIVOS DE RED.

2.2.1 ADMINISTRACIÓN DE RECURSOS.

Con la disponibilidad y la potencia de los equipos personales actuales, puede que se pregunte por qué son necesarias las redes. Desde las primeras redes hasta los equipos personales actuales de altas prestaciones, la respuesta sigue siendo la misma: las redes aumentan la eficiencia y reducen los costos. Las redes de equipos alcanzan estos objetivos de tres formas principales:

- Compartiendo información (o datos).

- Compartiendo hardware y software.
- Centralizando la administración y el soporte.

De forma más específica, los equipos que forman parte de una red pueden compartir:

- Documentos (informes, hojas de cálculo, facturas, etc.).
- Mensajes de correo electrónico.
- Software de tratamiento de textos.
- Software de seguimiento de proyectos.
- Ilustraciones, fotografías, vídeos y archivos de audio.
- Transmisiones de audio y vídeo en directo.
- Impresoras.
- Faxes.
- Módems.
- Unidades de CD-ROM y otras unidades removibles, como unidades Zip y Jaz.
- Discos duros.

Y existen más posibilidades para compartir. Las prestaciones de las redes crecen constantemente, a medida que se encuentran nuevos métodos para compartir y comunicarse mediante los equipos.

[Texto tomado de : http://fmc.axarnet.es/redes/tema_04.htm]

2.2.1.1 COMPARTIR INFORMACIÓN (O DATOS)

La capacidad de compartir información de forma rápida y económica ha demostrado ser uno de los usos más populares de la tecnología de las redes. Hay informes que afirman que el correo electrónico es, con diferencia, la principal actividad de las personas que usan Internet. Muchas empresas han invertido en redes específicamente para aprovechar los programas de correo electrónico y planificación basados en red.

Al hacer que la información esté disponible para compartir, las redes pueden reducir la necesidad de comunicación por escrito, incrementar la eficiencia y hacer que prácticamente cualquier tipo de dato esté disponible simultáneamente para cualquier usuario que lo necesite.

2.2.1.2 COMPARTIR HARDWARE Y SOFTWARE

Antes de la aparición de las redes, los usuarios informáticos necesitaban sus propias impresoras, trazadores y otros periféricos; el único modo en que los usuarios podían compartir una impresora era hacer turnos para sentarse en el equipo conectado a la impresora.

Las redes hacen posible que varias personas compartan simultáneamente datos y periféricos. Si muchas personas necesitan usar una impresora, todos pueden usar la impresora disponible en la red.

Las redes pueden usarse para compartir y estandarizar aplicaciones, como tratamientos de texto, hojas de cálculo, bases de datos de existencias, etc., para asegurarse de que todas las personas de la red utilizan las mismas aplicaciones y las mismas versiones de estas aplicaciones. Esto permite compartir fácilmente los documentos, y hace que la formación sea más eficiente.

2.2.1.3 CENTRALIZACIÓN DE LA ADMINISTRACIÓN Y EL SOPORTE

La conexión en red de los equipos también puede facilitar las tareas de soporte. Para el personal técnico, es mucho más eficiente dar soporte a una versión de un sistema operativo o aplicación y configurar todos los equipos del mismo modo que dar soporte a muchos sistemas y configuraciones individuales y diferentes.

2.2.2 REQUISITOS DE SEGURIDAD.

Los requisitos de seguridad de un sistema dado definen lo que significa la seguridad, para ese sistema.

Los requisitos sirven de base para determinar si el sistema implementado es seguro:

- Sin una serie de requisitos precisos tiene poco sentido cuestionar la seguridad de un sistema.

- Si los requisitos están débilmente establecidos no dicen mucho sobre la verdadera seguridad del sistema.

Algunos ejemplos de formulación de los requisitos de seguridad son los siguientes:

Directiva DOD 5200.28 (EE. UU.):

- Especifica cómo debe manipularse la información clasificada en sistemas de procesamiento de datos.

Manual de Referencia de Tecnología de Seguridad de la Computadora (EE. UU.):

- Especifica cómo evaluar la seguridad de los sistemas de computación de la Fuerza Aérea.

Ley de Intimidad de 1974 (EE. UU.):

- Requiere que las Agencias Federales aseguren

2.2.3 SEGURIDAD E INTEGRIDAD DE DATOS.

Seguridad en las redes son temas de discusión hoy en día en las corporaciones que utilizan estas herramientas para la transmisión de información. Algunas veces los equipos de administración de las empresas no están al tanto de los avances e

innovaciones de la Internet y la tecnología que conlleva. Sin este conocimiento las empresas no pueden tomar ventaja completa de los beneficios y capacidades de una red.

La seguridad en cada empresa tiene diferentes requerimientos, diferentes características, culturas diferentes y una infraestructura tecnológica distinta. En las múltiples organizaciones se tienen diferentes requerimientos para almacenar, enviar y comunicar información de manera electrónica.

La seguridad en el ámbito de la computación o bien la llamada seguridad informática, se puede dividir en diversas ramas: seguridad de software y sistemas operativos, seguridad física, seguridad de hardware, seguridad de acceso y la seguridad en redes. Esta última será la más analizada y estudiada, ya que es un elemento crucial en la creación de los diseños de sistemas de información.

La seguridad en redes es la seguridad que se aplica en los componentes de red de la organización. Se puede definir también como los procesos necesarios en la implementación de políticas de seguridad y mantenimiento de los dispositivos de una red.

Los elementos que se pueden emplear para brindar seguridad de redes en una organización pueden ser muy diversos y adaptables, cada empresa es diferente en sus necesidades. A la diversidad también se le puede agregar variabilidad, ya que se pueden

emplear de manera conjunta diversos equipos para que trabajen a fin de conseguir un objetivo en común. Un esquema de seguridad tiene que ser adaptable y variable, es decir se le pueden eliminar y agregar ciertos elementos sin comprometer los requerimientos de seguridad en su totalidad; así mismo, se puede implementar un esquema de seguridad sin modificar la topología de red que una organización estaba empleando previamente.

Existen diversas herramientas que pueden ser implementadas a fin de proveer seguridad en una red. Las aplicaciones de software y el hardware que proveen seguridad a una red de cómputo, necesitan interactuar con otros mecanismos para poder brindar los niveles necesarios de integridad que una corporación requiere.

Para que un sistema sea seguro debe cumplir con los requerimientos de Confiabilidad, Disponibilidad e Integridad. Como una categoría de la disponibilidad se mencionan: autentificación, autorización y acceso, AAA por sus significados en inglés (Authentication, Authorization and Accounting).

Confiabilidad es la parte que asegura que la información sólo puede ser vista y utilizada por las partes que están autorizadas. La comunicación entre partes confiables se establece una vez que se ha realizado el proceso de autentificación.

Disponibilidad se refiere a que la información está en todo momento a través de un medio seguro para los usuarios que la requieran, siempre y cuando tengan los recursos y accesos necesarios. Se tendrá acceso a la información siempre y cuando el que requiera ésta tenga previa autentificación los permisos y acreditaciones.

Integridad es saber que la información enviada no ha sido alterada, modificada o eliminada en el transcurso del camino.

Autentificación es simplemente asegurarse que lo usuarios son en realidad quien dicen ser. Cuando se utilizan recursos o se envían mensajes en una red privada amplia, sin mencionar la Internet, la autentificación es lo más importante.

Autorización cada uno de los usuarios podrá acceder solamente a los recursos de red que le fueron permitidos. Ningún usuario puede hacer uso de aplicaciones que no le han sido asignadas y tampoco se pueden auto asignar derechos, recursos y tareas.

Control de Acceso.

Esto quiere decir que cada usuario tiene un registro de los accesos a la red de la organización, de manera que se pueda monitorear la información a la que se ingresa y las aplicaciones que son empleadas. En caso que se detecten anomalías en el acceso, los recursos de red serán suprimidos.

Una característica de seguridad que se logra con los conceptos anteriores es el No Repudio en la información. El receptor de información debe estar completamente seguro de que la otra parte ya envió los datos. Sin la garantía mencionada, muchos de los negocios que necesitan confirmación no podrían existir. A través de la red se pueden emplear certificados digitales como medida de autentificación hacia algún usuario o una empresa. De igual forma, firmas digitales pueden ser empleadas, de manera que el receptor tenga una prueba de la persona que ha enviado información. Estos tipos de elementos son empleados para que la información enviada no sufra de negación o repudio.

2.2.4 DESARROLLO DE UNA POLÍTICA DE SEGURIDAD.

Para el funcionamiento de un esquema de seguridad, no sólo se necesitan los medios o dispositivos físicos; también es necesario implementar las normas de cómo se utilizarán los recursos y clientes pertenecientes a una red. La forma de operar de una red quedará explícita en una política de seguridad.

La primera regla de una política de seguridad en una red corporativa es que todo lo que no está expresamente permitido está prohibido. Una buena política de seguridad niega a un usuario el acceso a todas las secciones de la red, y luego otorga permiso a determinadas áreas en específico.

La implementación de una estrategia de seguridad comprende: la identificación de los bienes de la organización, identificación de amenazas, conocimiento de riesgos y vulnerabilidades, implementación de herramientas y tecnologías disponibles y una política de uso.

Uno de los primeros pasos en el establecimiento de una política es la identificación de las pertenencias de una empresa que necesiten estar protegidas, como son:

- Hardware, que incluye CPU's, monitores, terminales, estaciones de trabajo, servidores, impresoras, líneas de comunicación, etc.
- Software: programas fuente, utilerías, sistemas operativos, programas de comunicación y diagnóstico, etc.
- Información: bases de datos, archivos fuera de línea, respaldos, discos duros, etc.
- Documentación: manuales, procedimientos, esquemas, planos, etc.
- El análisis de riesgos determina lo que debe ser protegido y cómo debe ser protegido. Identificando como posibles agentes de riesgo para la red:
- Accesos no autorizados.
- Servicios no disponibles.
- Virus.
- Divulgación de información sensible a personas ajenas a la corporación. Ataque internos por parte de empleados.

La mayoría de los sistemas operativos almacenan información en archivos de registro. La verificación de estos archivos en una base de datos, puede ser una manera de prevenir un acceso no autorizado en el sistema. Algunos comandos de los sistemas operativos enlistan las aplicaciones que se están ejecutando en determinado momento, por lo que se pueden analizar y detectar los programas que no estén autorizados para correr.

Las políticas de uso de los equipos pueden contrarrestar muchos de los ataques que llevan a cabo hackers. Los métodos de ingreso a la red no deben ser dados a conocer a todos los usuarios, finalmente un cliente o usuario final requiere sólo el saber que su información se esta transmitiendo en forma segura.

Dentro de la política de seguridad se establecerán las normas para que un usuario se pueda conectar a la red, ya sea desde la organización misma o desde una localidad remota; algunas de las normas pueden ser:

- Establecimiento aleatorio de password o tokens.
- Acceso mediante equipos registrados en la organización.
- Instalación de clientes remotos.
- Monitoreo de tráfico.
- Duración de sesiones.

- Tiempo de vida de certificados.
- Descarga y ejecución de archivos.

El establecer una política de seguridad informática depende de las necesidades y capacidades de una corporación. Un buen esquema de seguridad no se basa en las últimas tecnologías ni en los recursos más caros, se establece en base a un control de equipos y en una buena administración de usuarios.

2.2.4.1 ELEMENTOS DE SEGURIDAD EN REDES.

El elemento más obvio en una política seguridad es la seguridad física, entendiéndose por ésta, el acceso restringido a los componentes mas sensibles de la red, como: los servidores, bases de datos, ERP's, dispositivos de almacenamiento masivo, entre otros.

Los equipos que almacenan la información y los dispositivos que se encargan de establecer las comunicaciones principales, deben ser operados sólo por personal autorizado y calificado.

Algunos de los elementos que ayudan en la implementación de seguridad en redes son descritos en las páginas siguientes.

Firewalls.

Los sistemas de firewall ofrecen protección una red a diferentes niveles, son configuraciones de hardware y software que establecen un perímetro entre la red de una corporación y la Internet, controlando el acceso de entrada y salida de la red. Estos sistemas permiten la ejecución de correos electrónicos y otras aplicaciones como la transferencia de archivos (FTP) y accesos remotos. Por otro lado pueden limitar el acceso a la red interna o bloquear cierto tipo de funciones por parte de los usuarios. Son un filtro para aplicaciones, e información tanto externas como internas.

Los sistemas de firewall proveen mecanismos de autorización que aseguran que un número limitado de usuarios o aplicaciones tengan acceso a la red de la corporación. El mecanismo de seguridad mencionado ofrece una translación de direcciones, lo cual protege el nombre y la dirección de cualquier máquina que se quiera comunicar a través de firewall.

Los firewall también pueden ser utilizados dentro de la red de una organización para segmentar servidores e incluso la red misma., de manera que se pueda tener un mejor registro de acceso y una mayor administración.

Password.

Los passwords o palabras secretas son una forma de identificar y autentificar a los usuarios de manera que estos ingresan a un sistema de información.

Desafortunadamente hay una infinidad de maneras de comprometer la integridad de un password. Debido a que en ocasiones son palabras de extraño significado o sin significado, tienen que ser escritas en algún documento, pudiendo éste caer en manos ajenas, por citar algún ejemplo.

Una situación adecuada para autentificación de usuarios de acceso remoto es la generación de password de una sola sesión. Al iniciar la sesión en la red, se genera un password de manera aleatoria; el cual sólo será válido durante el tiempo que se establezca comunicación entre la Terminal y el servidor de la organización. Cuado la sesión caduca el password expira y nunca más vuelve a ser válido.

Una buena política en la generación de password es la creación de los mismos, con una mezcla de letras y números y un número mínimo de caracteres. Los password únicos basados en esquemas de respuesta de tareas, son creados en un dispositivo pequeño similar a una tarjeta de crédito. El password es enviado como parte del proceso de autentificación y validado en un servidor de password, el cual da acceso al sistema. Otros sistemas emplean partes humanas, las cuales son irrepetibles, como passwords (e.g. retina, huella digital, voz); los biométricos, así llamados estos últimos, ofrecen el mejor proceso de autentificación de usuarios.

Encripción.

La encripción es sencillamente el proceso para transformar información legible a información totalmente ilegible, a través de algoritmos o tablas de transformación. El objetivo principal es que sólo las personas autorizadas puedan leer este tipo de documentos aparentemente sin valor. Existen distintas técnicas de encripción que funcionan en distintos niveles del modelo OSI.

Los mecanismos de encripción dependen de llaves o password. Entre más largo sea un password, la información encriptada es más difícil de romper. Si bien hay muchos estándares para encriptar, estos se pueden clasificar en dos algoritmos principales:

- Algoritmo de llave privada (simétrico).
- Algoritmo de llave pública (asimétrico).

En el algoritmo de encripción de llave privada, se emplea la misma llave o clave tanto para encriptar como para descifrar. En este método se tiene que acordar la llave secreta entre dos partes y no se puede dar a conocer a un tercero. El problema recae principalmente en que se tiene que intercambiar la llave de manera que no quede expuesta; esto ocurre principalmente cuando las partes involucradas se encuentran ubicadas en puntos lejanos. DES, 3DES, RC4 son ejemplos de llave privada.

El algoritmo de llave pública funciona de manera distinta, dos llaves son creadas: una privada y una pública. La llave privada sirve para descifrar mensajes que sólo pueden ser cifrados con la llave pública. Como su nombre lo dice la llave privada es conocida por la gente, sin necesidad de comprometer la privacidad del mensaje o de la otra llave. Una de las ventajas de utilizar el algoritmo de llave pública es el uso de firmas digitales y certificados. RSA, Diffie Hellman son ejemplos de este tipo de algoritmo.

El algoritmo de encripción asimétrico no es adecuado para cifrar grandes cantidades de información, el proceso resulta muy lento; en lugar de esto, se emplea la encripción simétrica (llave privada). La encripción asimétrica es normalmente usada para el intercambio de la llave secreta que se emplea para la encripción de la información. PGP (Pretty Good Privacy) es un ejemplo de la combinación de estos dos algoritmos.

Las transformaciones de mensaje o simplemente "hash", son extractos de la información enviada a un usuario. Estas transformaciones se convierten en las huellas digitales de los documentos que necesitan se autentificados. Las firmas digitales se crean en conjunto con los hash, como pueden ser: MD2, MD4, MD5, SHA-1, SHA-2.
[Texto tomado de: http://www.htmlweb.net/seguridad/varios/firma_certificados.html]

2.2.5 ANÁLISIS Y COMPARACIÓN DE SISTEMAS OPERATIVOS DE RED.

2.2.5.1 SISTEMA OPERATIVO UNIX

Los sistemas operativos UNIX desarrollados en los Laboratorios Bell se cuentan entre los éxitos más notables en el campo de los sistemas operativos. Los sistemas UNIX ofrecen un ambiente amable para el desarrollo de programas y el procesamiento de textos. Brindan facilidad para combinar unos programas con otros, lo cual sirve para fomentar un enfoque modular, de piezas de construcción y orientado a las herramientas, para el diseño de programas. Una vez transportado un sistema operativo UNIX a otra máquina, un enorme acervo de programas de utilidad general queda disponible en la máquina de destino.

El sistema operativo UNIX de 1981 era un sistema de tecleo intensivo que requería una larga lista de mandatos con diversas sintaxis. La generación más reciente de sistemas UNIX ofrece en muchos casos interfaces amab les con el usuario, orientadas al uso de ratón y de ventanas tales como X Window System de MIT, NeWS de Sun Microsystem y Open Look de AT&T.

Los sistemas UNIX se han convertido en los sistemas operativos para computadora personal preferidos por los usuarios de potencia, y es probable que lo mismo suceda con millones de usuarios más.

Casi todos los fabricantes importantes de computadoras ofrecen en la actualidad alguna forma de sistemas UNIX. Muchas compañías que habían estado ofreciendo sistemas UNIX además de sus propios sistemas, ahora promueven los sistemas UNIX dándoles por lo menos igual importancia.

2.2.5.1.1 CONCEPTO

Es un sistema operativo de tiempo compartido, controla los recursos de una computadora y los asigna entre los usuarios. Permite a los usuarios correr sus programas. Controla los dispositivos de periféricos conectados a la máquina.

2.2.5.1.2 CARACTERÍSTICAS GENERALES:

- Fue desarrollado por los Laboratorios Bell en 1969.
- El sistema operativo UNIX era, en 1981, un sistema de comando por línea, con varias opciones de sintaxis.
- El sistema operativo, ahora soporta ratón e interfaz de ventanas como X-Window System de MIT, News de Sun Microsystem y Open Look de AT&T.

2.2.5.1.3 CARACTERÍSTICAS ESPECÍFICAS:

- Es un sistema operativo multiusuario, con capacidad de simular multiprocesamiento y procesamiento no interactivo.
- Está escrito en un lenguaje de alto nivel : C.
- Dispone de un lenguaje de control programable llamado SHELL.
- Ofrece facilidades para la creación de programas y sistemas y el ambiente adecuado para las tareas de diseños de software.
- Emplea manejo dinámico de memoria por intercambio o paginación.
- Tiene capacidad de interconexión de procesos.
- Permite comunicación entre procesos.
- Emplea un sistema jerárquico de archivos, con facilidades de protección de archivos, cuentas y procesos.
- Tiene facilidad para redireccionamiento de Entradas/Salidas.
- Garantiza un alto grado de portabilidad.

El sistema se basa en un Núcleo llamado Kernel, que reside permanentemente en la memoria, y que atiende a todas las llamadas del sistema, administra el acceso a los archivos y el inicio o la suspensión de las tareas de los usuarios.

La comunicación con el sistema UNIX se da mediante un programa de control llamado SHELL. Este es un lenguaje de control, un intérprete, y un lenguaje de programación,

cuyas características lo hacen sumamente flexible para las tareas de un centro de cómputo. Como lenguaje de programación abarca los siguientes aspectos:

- Ofrece las estructuras de control normales: secuenciación, iteración condicional, selección y otras.
- Paso de parámetros.
- Sustitución textual de variables y Cadenas.
- Comunicación bidireccional entre órdenes de shell.

El shell permite modificar en forma dinámica las características con que se ejecutan los programas en UNIX:

Las entradas y salidas pueden ser redireccionadas o redirigidas hacia archivos, procesos y dispositivos; es posible interconectar procesos entre sí.

Diferentes usuarios pueden "ver" versiones distintas del sistema operativo debido a la capacidad del shell para configurar diversos ambientes de ejecución. Por ejemplo, se puede hacer que un usuario entre directamente a su sección, ejecute un programa en particular y salga automáticamente del sistema al terminar de usarlo.

2.2.5.2 SISTEMA OPERATIVO WINDOWS NT

Windows NT es un sistema operativo que ayuda a organizar la forma de trabajar a diario con la PC. Las letras NT significan Nueva Tecnología. Fue diseñado para uso de compañías grandes, por lo tanto realiza muy bien algunas tareas tales como la protección por contraseñas

Windows actúa como su ejecutivo personal, personal de archivo, mensajeros, guardias de seguridad, asistentes administrativos y mantenimiento de tiempo completo.
Quiere dar la impresión de ser su escritorio, de manera que encuentre en pantalla todo lo que necesite, gracias a su interfaz gráfica con iconos de colores y dibujos.

Lo que Windows NT no hace bien son los juegos y la multimedia, ya que no ha sido creado para tales usos.

2.2.5.2.1 VENTAJAS DE WINDOWS NT:

- La instalación es muy sencilla y no requiere de mucha experiencia.
- Multitarea.
- Multiusuario.
- Apoya el uso de múltiples procesadores.
- Soporta diferentes arquitecturas.
- Permite el uso de servidores no dedicados.
- Soporta acceso remoto.

- Ofrece mucha seguridad en sesiones remotas.
- Brinda apoyo a la MAC.
- Apoyo para archivos de DOS y MAC en el servidor.
- El sistema está protegido del acceso ilegal a las aplicaciones en las diferentes configuraciones.
- Ofrece la detección de intrusos.
- Permite cambiar periódicamente las contraseñas.
- Soporta múltiples protocolos.
- Carga automáticamente manejadores en las estaciones de trabajo.
- Trabaja con impresoras de estaciones remotas.
- Soporta múltiples impresoras y asigna prioridades a las colas de impresión.
- Muestra estadísticas de Errores del sistema, Caché, Información Del disco duro, Información de Manejadores, No. de archivos abiertos, Porcentaje de uso del CPU, Información general del servidor y de las estaciones de trabajo, etc.
- Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios.
- Permite realizar diferentes tipos de auditorias, tales como del acceso a archivos, conexión y desconexión, encendido y apagado del sistema, errores del sistema, información de archivos y directorios, etc.
- No permite criptografía de llave pública ni privada.

- No permite realizar algunas tareas en sesiones remotas, como instalación y actualización.

2.2.5.2.2 DESVENTAJAS DE WINDOWS NT:

- Tiene ciertas limitaciones por RAM, como; No. Máximo de archivos abiertos y almacenamiento de disco total.
- Requiere como mínimo 16 Mb en RAM, y procesador Pentium a 133 MHz o superior.
- El usuario no puede limitar la cantidad de espacio en el disco duro.
- No soporta archivos de NFS.
- No ofrece el bloqueo de intrusos.
- No soporta la ejecución de algunas aplicaciones para DOS.

2.2.5.3 SISTEMA OPERATIVO NETWARE DE NOVELL

El sistema de redes más popular en el mundo de las PCs es Netware de Novell. Este sistema se diseñó con la finalidad de que lo usarán grandes compañías que deseaban sustituir sus enormes máquinas conocidas como mainframe por una red de PCs que resultara más económica y fácil de manejar.

Netware es una pila de protocolos patentada y se basa en el antiguo Xerox Network System, XNS O pero con varias modificaciones. Netware de Novell es previo a OSI y no se basa en él, si acaso se parece más a TCP/IP que a OSI.

Las capas física y de enlace de datos se pueden escoger de entre varios estándares de la industria, lo que incluye Ethernet, el token ring de IBM y ARCnet. La capa de red utiliza un protocolo de interred poco confiable, si n conexión llamado IPX. Este protocolo transfiere paquetes de origen al destino en forma transparente, aun si la fuente y el destino se encuentran en redes diferentes. En lo funcional IPX es similar a IP, excepto que usa direcciones de 10 bytes en lugar de direcciones de 4 bytes.

Por encima de IPX está un protocolo de transporte orientado a la conexión que se llama NCP (Network Core Protocol, Protocolo Central de Red). El NCP proporciona otros servicios además del de transporte de datos de u suario y en realidad es el corazón de NetWare. También está disponible un segundo protocolo, SPX, el cual solo proporciona transporte. Otra opción es TCP. Las aplicaciones pueden seleccionar cualquiera de ellos.

Por ejemplo, el sistema de archivos usa NCP y Lotus NotesÒ usa SPX. Las capas de sesión y de presentación no existen. En la capa de aplicación están presentes varios protocolos de aplicación.

La clave de toda la arquitectura es el paquete de datagrama de interred sobre el cual se construye todo lo demás. El campo Suma de verificación pocas veces s e usa puesto que la capa de enlace subyacente también proporciona una suma de verificación. El campo Longitud del paquete indica qué tan grande es el paquete, es decir suma el encabezado más datos y el resultado se guarda en 2 bytes. El campo Control de transporte cuenta cuántas redes ha atravesado el paquete; cuando se excede un máximo, el paquete se descarta. El campo Tipo de paquete sirve para marcar varios paquetes de control. Cada una de las dos direcciones c ontiene un número de red de 32 bits, un número de máquina de 48 bits (La dirección 802 LAN) y la dirección local (Socket) de 16 bits en esa máquina. Por último se tienen los datos que ocupan el resto del pa quete, cuyo tamaño máximo está determinado por la capa subyacente.

2.2.5.3.1 VENTAJAS DE NETWARE:

- Multitarea
- Multiusuario.
- No requiere demasiada memoria RAM, y por poca que tenga el sistema no se ve limitado.
- Brinda soporte y apoyo a la MAC.
- Apoyo para archivos de DOS y MAC en el servidor.
- El usuario puede limitar la cantidad de espacio en el disco duro.
- Permite detectar y bloquear intrusos.

- Soporta múltiples protocolos.
- Soporta acceso remoto.
- Permite instalación y actualización remota.
- Muestra estadísticas generales del uso del sistema.
- Brinda la posibilidad de asignar diferentes permisos a los diferentes tipos de usuarios.
- Permite realizar auditorias de acceso a archivos, conexión y desconexión, encendido y apagado del sistema, etc.
- Soporta diferentes arquitecturas.
- Desventajas de NetWare.
- No cuenta con listas de control de acceso (ACLs) administradas en base a cada archivo.
- Algunas versiones no permiten criptografía de llave pública ni privada.
- No carga automáticamente algunos manejadores en las estaciones de trabajo.
- No ofrece mucha seguridad en sesiones remotas.
- No permite el uso de múltiples procesadores.
- No permite el uso de servidores no dedicados.

2.3 ATAQUES GENÉRICOS A SISTEMAS OPERATIVOS

Los principales ataques genéricos a los S. O. son los siguientes:

2.3.1 ASINCRONISMO:

- Se tienen procesos múltiples que progresan asincrónicamente.
- Un proceso podría modificar los parámetros ya validados por otro proceso pero aún no utilizados.
- Un proceso podría pasar valores malos a otro aún cuando el segundo realice una verificación extensa.

2.3.2 RASTREO:

- Un usuario revisa el sistema intentando localizar información privilegiada.

2.3.3 ENTRE LÍNEAS:

- Se utiliza una línea de comunicaciones mantenida por un usuario habilitado que está inactivo.

2.3.4 CÓDIGO CLANDESTINO:

- Se modifica el S. O. bajo una presunta depuración pero se incorpora código que permite ingresos no autorizados.

2.3.5 PROHIBICIÓN DE ACCESO:

- Un usuario escribe un programa que bloquea el acceso o servicio a los usuarios legítimos mediante:
    - Caídas del sistema, ciclos infinitos, monopolio de recursos, etc.

2.3.6 PROCESOS SINCRONIZADOS INTERACTIVOS:

- Se utilizan las primitivas de sincronización del sistema para compartir y pasarse información entre sí.

2.3.7 DESCONEXIÓN DE LÍNEA:

- El intruso intenta acceder al trabajo de un usuario desconectado:
    - Luego de una desconexión de línea.
    - Antes de que el sistema reconozca la desconexión.

2.3.8 DISFRAZ:

- El intruso asume la identidad de un usuario legítimo luego de haber obtenido la identificación apropiada por medios clandestinos.

2.3.9 ATAQUE "NAK":

Si el S. O. permite a un usuario:

- Interrumpir un proceso en ejecución mediante una *"tecla"* de *"reconocimiento negativo"*.
- Realizar otra operación.
- Reanudar el proceso interrumpido.
- Un intruso podría *"encontrar"* al sistema en un estado no protegido y hacerse con el control.

2.3.10 ENGAÑO AL OPERADOR:

- Con un engaño se hace realizar al operador una acción que comprometa la seguridad del sistema.

2.3.11 PARÁSITO:

- Mediante equipamiento especial el intruso:
    - Intercepta los mensajes entre un usuario habilitado y el procesador.
    - Los modifica o reemplaza totalmente.

2.3.12 CABALLO DE TROYA:

- El intruso coloca un código dentro del sistema que luego le permita accesos no autorizados.
- Puede permanecer en el sistema.
- Puede borrar todo rastro de sí mismo luego de la penetración.

2.3.13 PARÁMETROS INESPERADOS:

- El intruso suministra valores inesperados a una llamada al núcleo.
- Intenta aprovechar una debilidad de los mecanismos de verificación de la legalidad del S. O.

[Testo tomado de :

http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/SO14.htm]

3. EVALUACIÓN DE SOLUCIONES Y PLATAFORMAS DE ANTIVIRUS Y SPAMING

Con el correo electrónico sólidamente establecido como la aplicación clave de la empresa moderna, y el crecimiento exponencial en el volumen de tráfico de correo, sea éste correo deseado o no deseado y sumados a la enorme amenaza que representan los diversos virus, caballos de Troya y gusanos. Han puesto a los administradores de redes y de correo electrónico a enfrentar un gran reto; garantizar la integridad de los mensajes electrónicos e impedir los ataques a la seguridad que cada vez más se producen a través de ésta vía el "e-mail".

Para protegerse de estas amenazas se requieren de estrategias y técnicas para evitar violaciones a la seguridad de nuestra empresa. Surgen entonces software especializados en proteger y controlar el tráfico de correo electrónico que ingresa o sale de nuestro perímetro de la red. A éste software los conocemos como antivirus y antispam.

Existen programas antivirus que dan protección para cada nivel o capa de nuestra red informática, como detallamos a continuación:

- Protección perimetral para firewalls corporativo.

- Protección para navegación Web (proxies).
- Protección para gateway de correo SMTP .
- Protección para servidores de mensajería.
- Protección para servidores de archivos.
- Protección para estaciones de trabajo.

Hemos mencionado la existencia de las protecciones para todas éstas capas de nuestra red informática. Pero objetivo de este trabajo es enfocar un análisis en software antivirus para servidores de correo electrónico y principalmente el de Gateway o pasarelas de correo SMTP.

Cabe también indicar que la protección ideal para una empresa sería proteger con un software antivirus a cada capa de nuestra red informática.

3.1 CLASIFICACIÓN DE SOLUCIONES ANTIVIRUS Y SPAM

Está clasificación la hemos realizado basándonos en los diferentes tipos de soluciones que existen para cada parte o segmento de nuestra red informática

- Las soluciones antivirus de escritorio
- Las soluciones basadas en Gateway de correo electrónico
- Las soluciones basadas en servidor de correo electrónico

3.2 SOLUCIONES BASADAS EN ANTIVIRUS DE ESCRITORIO

Son soluciones idóneas para proteger sus estaciones de trabajo de la difusión agresiva , masiva e instantánea de virus y otras amenazas de Internet como spam, contenidos violentos o improductivos, programas espía, ataques de hackers e intrusos y demás peligros frecuentes en la Red.

Las soluciones para estaciones de trabajo son protecciones individuales y necesarias que forman parte de la protección ideal en una empresa, pero que adicional a estas deben establecerse mecanismos de seguridad en capas de la red superiores para así lograr una protección ideal en toda la organización

3.2.1 DIAGRAMA DE SOLUCIÓN BASADO EN ANTIVIRUS DE ESTACIONES TRABAJO

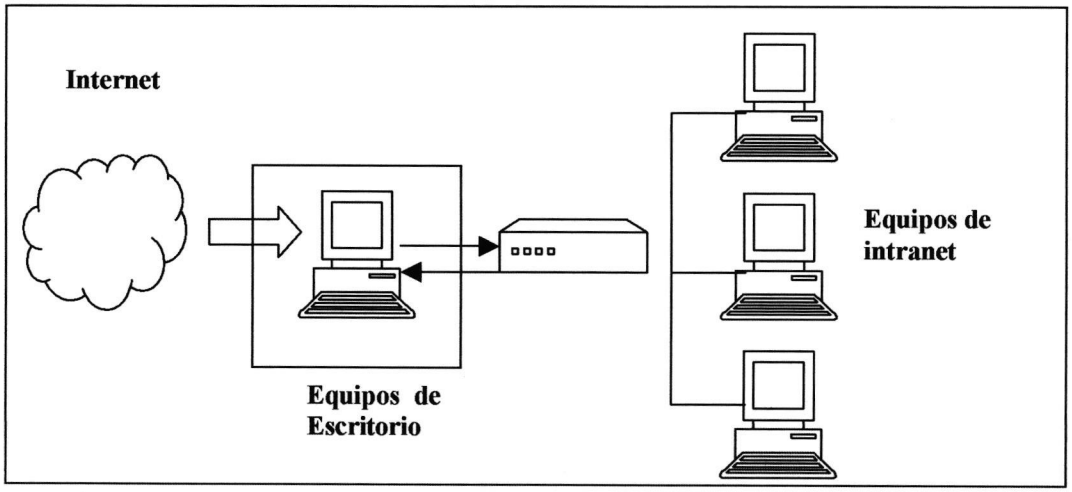


Diagrama 1: Cada estación de la red debe tener un Antivirus y Spam instalado

Diagrama 2: Ubicación por capas de los niveles de protección en una red.

[Gráfico tomado de: http://empresas.pandasoftware.es/productos/clientshield_tp/]

3.3 SOLUCIONES BASADAS EN SERVIDOR DE CORREO ELECTRÓNICO

Existen muchos productos en el mercado que realizan esta función de Servidor de correo electrónico. Entre los más populares tenemos :

- Microsoft Exchange Server
- Lotus Domino
- Novell Groupwise
- Sendmail

Los sistemas antivirus y antispam se han especializado para algunos de estos programas de correo electrónico. Sin embargo algunos sistemas de correo no poseen un programa antivirus que se especialice en ellos. Por lo general los sistemas antivirus sacan sus

productos tratando de dar soporte a aquellos software de correo que más sean utilizados o sea los más populares.

Por ésta razón el tema de ésta tesis se basa en el estudio de software antivirus y spam para servidores Mail Gateways que nos permita proteger nuestro servidor de correo de amenazas y vulnerabilidades informáticas que puedan venir en el correo electrónico sin importar que plataforma esté utilizando como servidor de correo electrónico.

3.3.1 DIAGRAMA DE SOLUCIÓN BASADA EN SERVIDOR DE CORREO ELECTRÓNICO

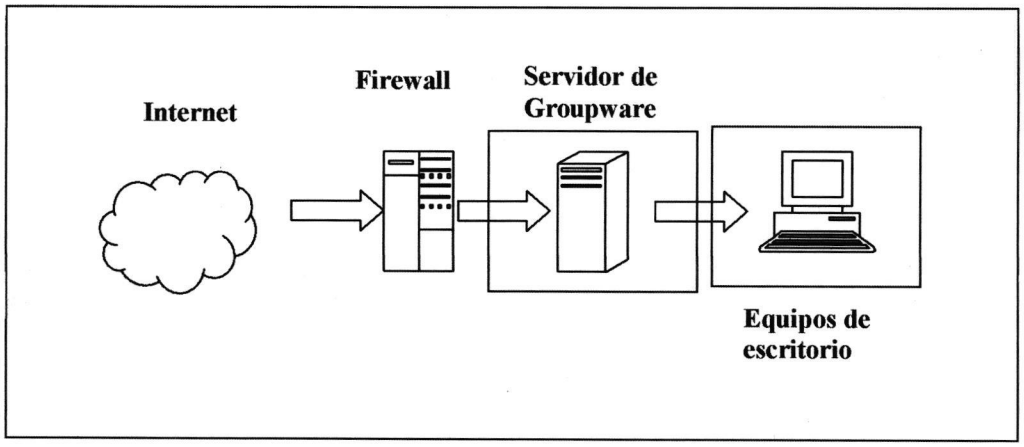


Diagrama 3:El servidor de correo tener instalado un Software antivirus y Spam

Diagrama 4: Ubicación por capas de los niveles de protección en la red

[Gráfico tomado de: http://empresas.pandasoftware.es/productos/exchangesecure/]

3.4 SOLUCIONES BASADAS EN GATEWAY DE CORREO ELECTRÓNICO

Los Gateway de correo electrónico independiente del Firewall nos proveen de una protección adicional muy importante actuando como un filtro del protocolo SMTP sin afectar a otros sistemas cuyas prestaciones son críticas como los servidores de correo.

Esto le permite mantener a su servidor de correo empresarial detrás de un cortafuegos, ya que el correo electrónico pasa por el gateway de correo SMTP que posee el software antivirus y antispam filtrándolo y protegiendo de ésta manera el servidor de correos

El Gateway de correo actuará como un equipo inteligente/servidor de retransmisión de correo en el perímetro de la red convirtiendo a la red que se encuentre detrás de esta pasarela en DMZ, zona desmilitarizada, y subred oculta.

3.4.1 DIAGRAMA DE SOLUCIÓN BASADA EN GATEWAY DE CORREO ELECTRÓNICO

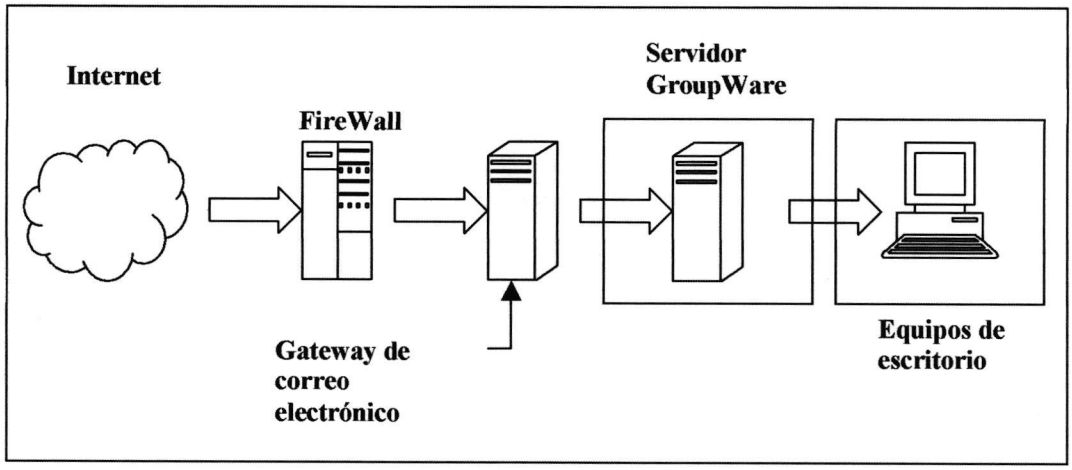


Diagrama 3: Servidor de correo se encuentra protegido por el Mail Gateway

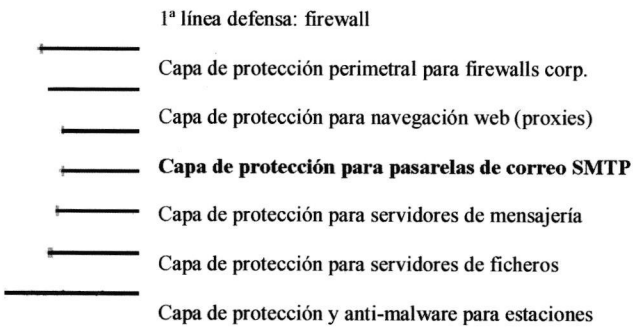


Diagrama 4: Ubicación por capas de los niveles de protección de una red

[Gráfico tomado de: http://empresas.pandasoftware.es/productos/sendmailsecure/]

3.4.2 VENTAJAS ADICIONALES

- Es totalmente independiente del software Groupware que tenga detrás del Gateway como servidor de correo.
- Puede realizar el mantenimiento de su servidor de Correo mientras continúa recibiendo correo de Internet.

- Utiliza menor recursos de su servidor de Correo debido a que el equipo que hace de Gateway de correo electrónico de Internet puede tener unas características técnicas menores que el equipo servidor de correo y procesar el correo más rápidamente .

- Tolerancia a fallos adicional ya que si algo ocurre con su servidor de correo usted continuará recibiendo correo, el cual se quedará encolado en el equipo Gateway.

3.4.3 DESVENTAJAS

- Se forman cuellos de botella y cuando el tráfico de correo es muy alto se debe implementar técnicas para hacer balanceo de carga.
- Debe instalarse un computador adicional en la red para configurarlo como mail Gateway .

- El servidor Gateway de SMTP solo se encarga del tráfico de correo SMTP y no POP3, IMAP, y acceso a sitios Webmail que también necesitan de protección.
- No da protección a la mensajería interna del Sistema de correo.

3.5 EVALUACIÓN DE SOFTWARE ANTIVIRUS

Existe un gran número de productos Antivirus y antispam actualmente en el mercado (ver anexo B). Sin embargo para efecto de está tesis se han seleccionado tres productos antivirus para detallar a continuación sus fortalezas y principales características. Esta selección se la ha realizado en base del siguiente criterio:

- El producto GFI por poseer diferentes motores antivirus incluidos en el. . Esto me da la seguridad que estoy utilizando un producto con mayor capacidad de detección.
- El producto de Symantec por se líder en la fabricación de software de seguridad
- El producto de Panda por ser un software para una plataforma diferente y potente como lo es Linux
- Otra característica por la que se ha seleccionado a estos productos es por que cada uno de ellos funciona en una plataforma diferente. El producto

GFI lo hace sobre la plataforma Windows. El producto de Symantec lo hace bajo Windows y Solaris y Panda lo hace sobre Linux

Estos productos seleccionados han sido galardonados y avalados por organismos especializados en la certificación de software de seguridad.

Ver Anexo A.

3.5.1 GFI MAILSECURITY FOR EXCHANGE / SMTP

Protege el correo electrónico de virus, abusos y Troyanos

GFI MailSecurity actúa como un Cortafuegos de Correo Electrónico y le protege de virus, debilidades y amenazas de correo, así como de los ataques por correo dirigidos a su organización.

GFI MailSecurity está disponible en versiones :

Gateway SMTP y para VS API.

La versión Exchange 2000 VS-API se integra estrechamente con Exchange Server 2000/2003 y analiza los almacenes de información de Exchange.

La versión Gateway SMTP debe implantarse en el perímetro de la red como servidor retransmisor de correo y analiza el correo entrante y saliente.

3.5.1.1 CARACTERÍSTICAS PRINCIPALES

Análisis/filtrado del contenido del correo

Utilizando el poderoso motor de reglas de GFI MailSecurity puede configurar sistemas de reglas basadas en el tipo de archivo y el usuario, que le permiten poner en cuarentena archivos peligrosos para aprobación administrativa. Todos los adjuntos ejecutables pueden ser puestos en cuarentena para revisión administrativa antes de que sean distribuidos a los usuarios.

GFI MailSecurity también busca contenido ofensivo y fugas de información, por ejemplo, un empleado enviando por correo una base de datos. También puede escoger eliminar los adjuntos, como archivos .mp3 o mpg.

Análisis de virus utilizando múltiples motores antivirus

GFI MailSecurity es independiente del motor antivirus, admitiendo la operación de múltiples motores antivirus simultáneamente. La tecnología "mejor de su clase" de GFI en el análisis de mensajes de Exchange, se puede combinar con uno o más motores antivirus "mejores de su clase", proporcionándole mucha más seguridad. Como cada motor antivirus tiene sus propios puntos fuertes y carencias, varios motores se complementan para proporcionar los más altos niveles de seguridad.

Analizador de Troyanos y ejecutables

El analizador de Troyanos y Ejecutables de GFI MailSecurity detecta ejecutables desconocidos y maliciosos (por ejemplo, Troyanos) analizando qué hace el ejecutable.

El Analizador de Troyanos y Ejecutables utiliza una técnica diferente basada en un análisis inteligente del nivel de riesgo del ejecutable. Esto lo hace descompilando el ejecutable, detectando en tiempo real que podría hacer, y comparando sus acciones con una base de datos de acciones maliciosas. El analizador pone en cuarentena cualquier ejecutable que realice actividades sospechosas, tales como acceso a un módem, activación de conexiones de red o acceso a la libreta de direcciones.

Están incluidos los motores antivirus Norman Virus Control y BitDefender

GFI MailSecurity se entrega junto con Norman Virus Control y BitDefender. Norman Virus Control es un potente motor antivirus que ha recibido el premio 100% Virus Bulletin 16 veces consecutivas. También tiene la certificación ICSA y Checkmark. BitDefender es un motor antivirus muy rápido y flexible que sobresale en el numero de formatos que reconoce y es capaz de escanear. BitDefender está certificado por ICSA y ha ganado los premios 100% Virus Bulletin y European Information Technologies Prize 2002. GFI MailSecurity actualiza automáticamente el archivo de definición de BitDefender con los nuevos que estén disponibles. El precio de GFI MailSecurity incluye las actualizaciones por un año.

Motores anti-virus Kaspersky y McAfee opcionales

Para adquirir aun mayor seguridad, los usuarios pueden incluir el motor anti-virus Kaspersky y/o McAfee como un tercer o cuarto motor o para reemplazar uno de los otros motores. Kaspersky Anti-Virus está certificado por ICSA y es bien conocido por la insuperable profundidad de su escaneo de objetos, el alto ratio en el que aparecen nuevas firmas de virus, y su tecnología heurística única que efectivamente neutraliza virus desconocidos. El motor anti virus McAfee es particularmente potente detectando ataques que no son virus como peligrosos controles ActiveX.

Motor de detección de debilidades de correo

El motor de detección de abusos de correo se construye en base a las avanzadas investigaciones de GFI sobre abusos de correo y le salvaguarda de futuros virus de correo y ataques que utilicen debilidades conocidas de aplicaciones o sistemas operativos. Por ejemplo, GFI MailSecurity le habría protegido frente a los virus Nimda y Klez la primera vez que surgieron sin necesidad de ninguna actualización, porque estos virus utilizan debilidades conocidas. GFI SecurityLabs encuentra regularmente nuevas debilidades de correo, y estas son automáticamente descargadas por GFI MailSecurity.

Eliminación automática de los scripts HTML

La llegada del correo HTML ha hecho posible para los hackers/creadores de virus el ejecutar comandos incrustados en el correo HTML. GFI MailSecurity busca código

script en el cuerpo del mensaje y deshabilita esos comandos antes de enviar el correo HTML "limpio" al destinatario. GFI MailSecurity es el único producto que le protege de los correos electrónicos HTML potencialmente maliciosos utilizando un proceso patentado por GFI, guardándole de virus HTML y de ataques lanzados vía correo HTML.

Aprobar/rechazar correo utilizando el cliente moderador, su cliente de correo o el moderador Web.

GFI MailSecurity proporciona diversas opciones de moderar el correo en cuarentena. El cliente moderador le proporciona el una interfaz Windows para aprobar/rechazar correo. El moderador Web le permite aprobar/rechazar los correos desde cualquier lugar de su red. Como alternativa, GFI MailSecurity también puede reenviar los correos en cuarentena a una dirección de correo, permitiéndole utilizar una carpeta pública para distribuir los elementos en cuarentena entre múltiples administradores.

Perfecta integración con Exchange Server 2000/2003 a través de VS API

GFI MailSecurity for Exchange utiliza el nuevo Virus Scanning API (VS API) de Exchange 2000/2003 para escanear el correo interno y prevenir así las amenazas internas de virus. Esta API está implementada a muy bajo nivel en el almacén de Exchange. Esto permite a GFI MailSecurity trabajar con un alto rendimiento y garantiza que el mensaje se analizará antes de que cualquier cliente pueda acceder al mensaje o

adjunto. GFI MailSecurity puede también escanear el correo interno, así como todo el correo entrante y saliente. GFI MailSecurity soporta :

- Examinador nativo de contenido MIME/MAPI
- Examinador avanzado y proactivo en segundo plano
- Encolamiento por prioridad y procesamiento de colas múltiple (multithreaded)
- Opciones de configuración de la base de datos por mensajería
- Registro de sucesos y contadores de rendimiento.

Microsoft anima encarecidamente el desarrollo y la adopción de soluciones de seguridad de contenido basadas en Exchange VS API. De hecho, Microsoft no soporta ninguna solución que no use VS API, lo que significa que el Soporte de Microsoft le sugiere que desinstale las soluciones de seguridad de contenido no basadas en VS API instaladas en Exchange Server.

Se puede implementar ambos modos SMTP Gateway y VS API

GFI MailSecurity le permite implementar la versión SMTP Gateway y la versión VS API simultáneamente. De esta forma, puede bloquear archivos adjuntos peligrosos a nivel de Gateway, sin interferir el intercambio interno de archivos. La versión VS API se puede utilizar para el control interno de las amenazas de virus y la detección de usuarios internos intentando atacar a otros usuarios mediante abusos de correo electrónico. GFI MailSecurity también bien le permite implementar ambas versiones.

Certificado por Checkmark e ICSA

GFI MailSecurity posee la certificación Checkmark de West Coast Labs y la certificación ICSA de TruSecure.

Enorme valor

GFI MailSecurity es el producto de chequeo de contenido y antivirus más rentable. La licencia estándar incluye un año completo de actualizaciones antivirus, así como 3 meses de soporte gratuito e ilimitado. El coste de las actualizaciones antivirus en el segundo año después de la compra es mínimo, aproximadamente el 15% del precio de compra, dependiendo del número de usuarios que haya adquirido.

Otras características:

- Cuarentena automática de documentos Microsoft Office con macros
- Detecta extensiones de archivos adjuntos ocultas y renombradas
- Configuración de reglas flexible y basadas en el usuario
- Escanea correos incrustados
- El motor de descompresión escanea más de 70 formatos de compresión
- Análisis léxico.

3.5.1.2 REQUERIMIENTOS TÉCNICOS

Modo Gateway

- Windows 2000/2003 - Pro, Server o Advanced Server - o Windows XP (Tenga en cuenta que si usa Windows 2000/2003 Pro o XP, solo podrá aceptar hasta 10 conexiones SMTP entrantes simultáneamente, por lo que recomendamos utilizar Windows 2000/2003 Server).
- Servicio SMTP de IIS5 instalado y funcionando como un retransmisor SMTP a su servidor de correo.
- Microsoft Exchange Server 2003, 2000, 4, 5 o 5.5, Lotus Notes 4.5 y superior, o un servidor de correo SMTP/POP3.

Modo VS API:

- Windows 2000/2003 Server o Advanced Server.
- Exchange 2003 o Exchange 2000 Server con SP1 o superior, recomendado Exchange SP 2.

3.5.1.3 PRECIOS

La experiencia de GFI en el desarrollo de seguridad de contenido de correo para Exchange Server, nos ha permitido hacer un software muy compacto y sencillo de implantar. Como GFI vende miles de unidades mensuales, somos capaces de mantener un precio muy bajo.

El precio incluye actualizaciones de virus por 1 año a partir de la compra, 3 meses de soporte gratis y 3 meses de upgrade.

GFI MailSecurity incluye el motor antivirus Norman y BitDefender y actualizaciones, y todas las actualizaciones del producto por 1 año.

		Price			**Price**
10 buzones	MSEC10	$ 295	250 buzones	MSEC250	$ 1595
25 buzones	MSEC25	$ 315	500 buzones	MSEC500	$ 2150
50 buzones	MSEC50	$ 525	1000 buzones	MSEC1000	$ 3250
100 buzones	MSEC100	$ 950	Buzones ilimitados	MSECUNL	$ 3750

Tabla 3.1 Lista de precios licencias de Norman y BitDefender

Los motores antivirus Kaspersky y/o McAfee son opcionales y pueden se agregados por un precio en la lista inferior.

		Price			**Price**
Up 25 buz.	KASP25	$ 99	500 buzones	KASP500	$ 695
50 buzones	KASP50	$ 185	1000 buzones	KASP1000	$ 950
100 buzones	KASP100	$ 270	2500 buzones	KASP2500	$ 1350
250 buzones	KASP250	$ 475	Buzones ilimitados	KASPUNL	$ 1995

Tabla 3.2 Lista de precios de licencias Kaspersky

		Price			Price
25 buzones	MCAFEE25	$ 100	500 buzones	MCAFEE500	$ 960
50 buzones	MCAFEE50	$ 195	1000 buzones	MCAFEE1000	$ 1075
100 buzones	MCAFEE100	$ 375	2500 buzones	MCAFEE250	$ 2495
250 buzones	MCAFEE250	$ 640	5000 buzones	MCAFEE5000	$ 4995

Tabla 3.3 Lista de precios de licencias McAfee

[Texto tomado de : http://www.gfihispana.com/es/mailsecurity/]

3.5.2 SYMANTEC MAIL SECURITY PARA SMTP

Seguridad integrada y de múltiples capas para el correo electrónico contra los virus y el Spam. Donde mejor se encuentran los virus, gusanos, caballos de Troya, Spam y otros contenidos no deseados de correo electrónico es fuera de la empresa, detenidos en el primer punto de entrada. Symantec Antivirus para SMTP Gateways ofrece seguridad integrada de múltiples capas para el tráfico de correo electrónico de Internet mediante el análisis de los virus y el bloqueo de los contenidos no deseados como spam, en las plataformas Windows y Solaris.

3.5.2.1 CARACTERÍSTICAS PRINCIPALES

Prevención de spam de múltiples capas combinando la detección heurística y de listas negras con listas blancas, para incrementar la detección y minimizar los falsos positivos.
Protección integrada de correo electrónico contra virus, spam y contenidos no deseados en el Gateway de correo electrónico (SMTP) y POP3 de Internet.

Combina la detección basada en firmas con tecnologías pro-activas de análisis heurístico para asegurar una protección confiable y rápida contra virus en el tráfico entrante y saliente, incluyendo los formatos de anexo comunes y los formatos de compresión.

Incluye tecnología de filtrado integrada para bloquear los contenidos de correo electrónico no deseados por dirección o dominio del remitente, asunto del mensaje, documento anexo y tamaño del mensaje.
Administración remota segura, avanzadas alertas de ataques e informes concisos para visualizar las medidas clave de rendimiento y análisis, además del estado general del sistema.

Respaldado por Symantec™ Security Response, la primera organización mundial en investigación y soporte de la seguridad en Internet.

Prevención de múltiples capas contra el Spam

El Spam (correo electrónico no solicitado) es una importante amenaza a los recursos empresariales de correo electrónico debido a que utiliza ancho de banda, ocupa espacio de almacenamiento del correo y afecta la productividad del usuario final. Con el Spam, como con los virus, cualquier línea de defensa individual está destinada a fracasar debido a la capacidad de innovación de sus creadores. Para obtener la mejor protección de largo plazo, es necesario contar con múltiples líneas de defensa.

Para combatir eficazmente esta amenaza y obtener un máximo de detección con un mínimo de falsos positivos, se requieren varias capas y técnicas de protección. Symantec Antivirus para SMTP Gateways es una solución antispam altamente integrada y de múltiples capas que detiene el Spam combinando métodos que incluyen la detección heurística antispam y soporte para múltiples servicios de lista negra en tiempo real. Otras de las capas incluyen listas de bloqueo de remitente personalizadas para bloquear por dominios de primer y segundo nivel y por direcciones de correo electrónico y soporte de listas blancas que permiten la corrección de falsos positivos y una prevención total. A través del enfoque de prevención de Spam de múltiples capas, Symantec Mail Security para SMTP Gateways proporciona flexibilidad para implementar medidas antispam eficaces a nivel del Gateway

3.5.2.2 REQUERIMIENTOS TÉCNICOS

SOLARIS

- Servidor basado en SPARC
- Solaris 8 o 9
- 512 MB de RAM como mínimo (se recomienda 1GB para mejor funcionamiento)
- 100 MB para la instalación
- 500 Mb como mínimo después de la instalación para procesar el correo
- Microsoft Internet Explorer 6.0 –o bien– Netscape Navigator 7.02 o superior

WINDOWS® NT/2000 SERVER

- Pentium® III ó IV de Intel® o compatible
- Windows 2003 Server o Windows 2000 Server con SP4
- 512 MB de RAM como mínimo
- 100 MB para la instalación
- 500 MB como mínimo después de la instalación para procesar el correo
- Microsoft Internet Explorer 6.0 o Netscape Navigator 7.02

[Texto tomado de : http://enterprisesecurity.symantec.com/products]

3.5.3 PANDA SENDMAILSECURE ANTIVIRUS

Panda Software ofrece a las organizaciones que utilizan este producto, SendmailSecure, una solución flexible que gracias a la tecnología MilterAPI, un interfaz de programación de la aplicación para la gestión de contenidos, dota a empresas y proveedores de Internet de una eficaz protección integrada y en tiempo real para todo el perímetro de la red.

3.5.3.1 CARACTERÍSTICAS PRINCIPALES

Flexible configuración de dominios y alertas

Las avanzadas opciones de configuración de SendmailSecure permiten aislar código infectado o sospechoso de contener virus, a un área segura de su equipo, al tiempo que se lo notifica al administrador, remitente o destinatario del mensaje. Sin embargo, la opción más potente que incluye el nuevo SendmailSecure es la posibilidad de configurar y seleccionar aquellos dominios y direcciones de correo que se desean analizar o excluir del análisis, lo que permite priorizar la protección en caso de saturación en el servidor.

Actualizaciones transparentes y progresivas

SendmailSecure se actualiza automáticamente y de forma transparente al menos una vez al día y sin que sea necesaria la intervención del administrador. Las actualizaciones

incrementales del fichero de firmas de virus contribuyen a la reducción del consumo total de ancho de banda y a suavizar los picos que se producen en las comunicaciones.

Administración centralizada y remota

Además de la tradicional consola web para gestionar las actualizaciones y monitorización de incidencias desde entornos heterogéneos, SendmailSecure cuenta con una nueva herramienta de administración bajo Windows, Panda AdminSecure.

Desde Panda AdminSecure se instalan y controlan desde un solo punto de forma remota todas las soluciones de Panda, contando para ello con vistas, informes, avisos, etc. en tiempo real. Al mismo tiempo, permite conocer el nivel de protección antivirus de cada servidor de correo conectado a la red.

Rendimiento optimizado

Su innovadora tecnología analiza en memoria todo tipo de ficheros comprimidos, obteniendo una velocidad de exploración muy superior a la de otros antivirus que necesitan desviarlos al disco duro. El resultado es un mayor rendimiento en el análisis y procesamiento de los mensajes.

Máxima protección de correo

SendmailSecure destaca por analizar y desinfectar virus dentro del cuerpo del mensaje independientemente de su formato: texto plano, texto enriquecido o formato HTML. La capacidad analítica del antivirus permite también inspeccionar archivos adjuntos y comprimidos, mensajes anidados e incluso objetos OLE incrustados en los mensajes.

SendmailSecure analiza la totalidad de los mensajes y es capaz de desinfectar virus comprimidos en formato ZIP y GZIP desde memoria, sin necesidad de descomprimirlos en el disco duro.

Tecnología de última generación

Además del motor antivirus de última generación de Panda, SendmailSecure emplea la tecnología MilterAPI, un interfaz de programación de la aplicación para la gestión de contenidos, lo que facilita su perfecta integración con los sistemas Linux bajo los que opera y lo convierte en la solución estándar para dichas plataformas.

La tecnología MilterAPI permite instalar SendmailSecure directamente en la máquina que aloja la pasarela SMTP, distribuir los filtros del producto antivirus en varias máquinas individuales a las que accede la pasarela SMTP principal o compartir los filtros instalados en una máquina entre varias pasarelas Sendmail.

3.5.3.2 REQUERIMIENTOS TÉCNICOS

- Procesador Pentium 200 MHz (o superior), con 64MB de memoria RAM y 90MB de espacio libre en disco duro. Sistema operativo para integración con AdminSecure o instalación independiente: Red Hat 7.0, 7.1, 7.2, 7.3, 8.0, 9.0 y Red Hat Enterprise, SUSE 7.3, 8.0, 8.2,9.0 ó 9.1 o Debian 3.0 (Woody).

- Otros sistemas operativos soportados para una instalación independiente: Red Hat 6.2 o Best Linux 2000.
- Servidor SMPT Sendmail versiones 8.11.3.
- Consola web: Internet Explorer 4.0 (o superior) o Netscape Navigator 4.6 (o superior).

Panda AdminSecure:

Pentium III 800 MHz. 512 MB RAM. 512 MB disco duro. Sistemas operativos: Windows NT4 SP6, 2000, XP y Server 2003 (Enterprise Edition).

3.5.3.3 PRECIOS

Panda SendmailSecure	$115.00. por servidor

[Texto tomado de: http://empresas.pandasoftware.es/productos/sendmailsecure/]

3.6 EVALUACIÓN DE SOFTWARE ANTISPAM

Correos electrónico fraudulentos, inapropiados y ofensivos están siendo enviados cada día en grandes cantidades a las empresas, por lo que una protección antispam es un componente esencial de la estrategia de seguridad de su red. El spam malgasta el tiempo

de los usuarios de la red y los recursos de la misma, y además puede llegar a ser peligroso.

El uso software de filtrado o bloqueo de spam es una importante y necesaria medida de seguridad para combatir este mal.

Hemos evaluado 3 diferentes productos que detallamos a continuación

3.6.1 GFI MAILESSENTIALS FOR EXCHANGE / SMTP

GFI MailEssentials afronta la protección Spam a nivel de servidor y elimina la necesidad de instalar y actualizar el software antispam en cada estación de trabajo.

GFI MailEssentials ofrece una rápida puesta en marcha y un alto ratio de detección de Spam utilizando análisis Bayesiano y otros métodos – No se requiere configuración, muy pocos positivos falsos mediante su lista blanca automática, y la habilidad de adaptarse automáticamente a su entorno de correo para constantemente afinar y mejorar la detección de Spam. GFI MailEssentials incluye además herramientas de administración de correo para su servidor de correo: avisos corporativos, archivo y supervisión, informes del correo de Internet, servidor de listas, auto respuestas basadas en servidor y descarga POP3.

3.6.1.1 CARACTERÍSTICAS PRINCIPALES

Antispam basado en servidor

GFI MailEssentials está basado en servidor y se instala en el servidor de correo o en el gateway, eliminando la molesta implantación y administración de productos antispam basados en cliente. Antispam en base al cliente supone enseñar a sus usuarios crear conjuntos de reglas antispam, y por lo tanto los usuarios tendrán que pasar tiempo actualizando estas reglas. Además, este sistema no previene que su servidor deje de almacenar mensajes Spam.

Tecnología de filtrado Bayesiano

El filtrado Bayesiano es ampliamente aclamado por destacados expertos y publicaciones como la mejor forma de atrapar el spam. Un filtro Bayesiano utiliza una aproximación matemática basada en el spam y ham conocidos (correo válido). Esto le da una tremenda ventaja sobre otras soluciones spam que sólo comprueban palabras clave o se fían en la descarga de firmas de spam conocido. El filtro Bayesiano de GFI utiliza una fórmula matemática avanzada y un conjunto de datos que están 'hechos a medida' para su instalación: Los datos spam son continuamente actualizados por GFI y son descargados automáticamente por GFI MailEssentials, mientras que los datos ham (correo válido) se recogen automáticamente de su correo saliente. Esto significa que el filtro Bayesiano está constantemente aprendiendo nuevos trucos spam, y significa que los spammers no pueden evitar el conjunto de datos utilizado. Esto resulta en más de un

98% de detección de spam, trás el necesario período de dos semanas de aprendizaje. En suma, el filtrado Bayesiano tiene las siguientes ventajas:

- Tiene en cuenta la totalidad del mensaje spam, no sólo palabras o firmas de spam conocido
- Aprende de su correo saliente (ham) y por lo tanto reduce mucho los positivos falsos.
- Se adapta con el paso del tiempo aprendiendo del nuevo spam y del nuevo correo válido
- El conjunto de datos es único para cada empresa, haciéndolo imposible de eludir
- Multilingüe e internacional.

Descarga actualizaciones para la base de datos del perfil spam

GFI MailEssentials puede descargar actualizaciones para la base de datos de perfil de spam Bayesiano desde el sitio de GFI, asegurando que reconoce el spam y las técnicas de Spaming más recientes. GFI mantiene la base de datos de perfiles spam trabajando con organizaciones de recogida de spam que suministran continuamente ejemplos.

Clasifica el spam en carpetas de correo basura de los usuarios

GFI MailEssentials le proporciona la flexibilidad de escoger qué hacer con el spam. Puede eliminarlo, moverlo a una carpeta, reenviar el correo spam a una dirección o carpeta de correo pública, o enviarlo a carpetas individuales personalizadas (por

ejemplo, una carpeta de "correo basura") en las bandejas de entrada de los usuarios. Esto permite a los usuarios revisar fácilmente el correo que ha sido marcado como spam.

Almacenamiento de correo en base de datos SQL

GFI MailEssentials puede archivar todo el correo entrante y saliente en una base de datos Microsoft SQL Server. Puede buscar un correo particular o toda una conversación mediante el interfaz web incluido. El archivo de correo es esencial por razones de copia de seguridad y búsqueda.

GFI MailEssentials se integra con Exchange y puede utilizar Microsoft Access o Microsoft SQL Server. Se soportan tanto listas de noticias como de discusión.

Fácil afinado del motor Bayesiano mediante carpetas públicas

Los administradores puede afinar sencillamente el motor Bayesiano arrastrando el spam o el ham a la carpeta pública adecuada. GFI MailEssentials aprende del spam y el ham que se recoge de estas carpetas y mejora su ratio de detección de spam. Los administradores pueden controlar el acceso a esta característica mediante el uso de la seguridad de Carpetas Públicas.

Permite a los usuarios poner en lista blanca o negra mediante carpetas públicas

GFI MailEssentials permite a los usuarios poner los remitentes en lista blanca o negra simplemente arrastrando el correo a una carpeta pública. Esto proporciona a los usuarios más control y reduce la administración. Los administradores pueden controlar el acceso a esta característica mediante el uso de la seguridad de Carpetas Públicas.

Análisis de cabecera y comprobación de palabras clave

GFI MailEssentials analiza inteligentemente la cabecera del correo e identifica el spam en base a la información de los campos del mensaje. Detecta cabeceras falsificadas, IPs codificadas, mutación de spam, spam enviado desde dominios no válidos, y más.

Además le permite configurar palabras clave para comprobar el spam utilizando el análisis de palabras clave.

Análisis de listas negras DNS de terceros (DNSBL)

GFI MailEssentials admite listas negras DNS de terceros (listas negras en tiempo real), que son bases de datos de spammers conocidos. Si el servidor de correo remitente está en una de estas listas, GFI MailEssentials marca el correo como spam. GFI MailEssentials soporta populares listas negras de terceros como ORDB, SpamHaus, Spamcop o RBL. GFI también soporta listas negras personalizadas.

La gestión automática de lista blanca reduce los positivos falsos

Las listas blancas le permiten asegurarse de que el correo de determinados remitentes o dominios nunca sea marcado como spam, permitiendo reglas anti-spam más rigurosas. GFI MailEssentials incluye una herramienta pendiente de patente de administración automática de lista blanca, que agrega automáticamente todos los socios de negocio a su lista blanca. Esto reduce enormemente los falsos positivos, son necesidad de administración adicional. Las listas blancas también se pueden construir en base a nombres de dominio, direcciones de correo y en base a palabras clave.

Informes sobre el spam filtrado y el uso del correo

El nuevo motor de informes basado en base de datos le permite crear informes avanzados de su correo entrante y saliente. Puede informarse de la cantidad de spam que filtró y qué reglas atraparon la mayoría del spam. También puede generar informes sobre usuarios, dominios y uso del servidor de correo.

Texto de renuncia/pie/cabecera para toda la empresa

GFI MailEssentials le permite incluir avisos al principio o final del correo. Se admiten los formatos texto y HTML. Puede incluir campos/variables para personalizar el aviso. También puede crear múltiples avisos y asociarlos con un usuario, grupo o dominio.

Soporte de SPF - el Marco Legal de Remitente

Como la mayoría de los spammers actuales parodian direcciones de correo, es importante poder comprobar si un correo es auténtico o si ha sido enviado desde una

dirección de correo falsificada. Este se puede hacer mediante el Marco Legal de Remitente (SPF), que permite a los usuarios comprobar si un correo particular se ha originado desde donde indica. GFI MailEssentials es uno de las primeras soluciones anti-spam comerciales en soportar este marco. Su nuevo módulo SPF comprueba automáticamente si el correo de una empresa particular fue enviado por sus servidores de correo registrados. Para conocer más sobre SPF,.

Elimina los ataques al directorio

A menudo los spammers intentan adivinar direcciones de destinatario generando múltiples direcciones aleatorias de un dominio; entonces envian su correo spam a todas esas direcciones. GFI MailEssentials comprueba la validez de todas las direcciones de correo incluidas en el correo enviado, mediante una consulta al Directorio Activo, y si no son todas válidas, clasifica el correo como spam.

Seguimiento de correo

La característica de seguimiento de correo le permite mantener un almacén central de todas las comunicaciones de correo de una persona o departamento determinado. Mediante la configuración de que el correo sea copiado a una dirección de correo, todo el correo puede ser almacenado en un almacén Exchange o Outlook, haciendo sencilla la búsqueda de correo o contenido.

Perfecta integración con Exchange 2000/2003 y 5.5

GFI MailEssentials se integra perfectamente con Microsoft Exchange 2000/2003: Se instala sobre el servicio Exchange SMTP y no necesita configuración de gateway. Mediante el protocolo SMTP, también trabaja con Exchange 5.5, Lotus Notes y otros populares servidores SMTP/POP3.

Otras características:

- Lista blanca basada en palabras clave
- Bloqueo de spam en idiomas extraños basado en juegos de caracteres
- Monitorización de las comunicaciones por correo de un usuario o departamento particular
- Informes de no entrega (NDRs) falsos
- Auto respuestas personalizados basadas en servidor con números de seguimiento
- Descargador POP3
- Interfaz web para la búsqueda de correo archivado.

3.6.1.2 REQUERIMIENTOS TÉCNICOS

- Windows 2000/2003 - Pro, Server o Advanced Server o Windows XP Professional.
- Servicio SMTP de IIS5 instalado y funcionando como un retransmisor SMTP a su servidor de correo.

- Microsoft Exchange server 2000, 2003, 4, 5 ó 5.5, Lotus Notes 4.5 y superior, o un servidor de correo SMTP/POP3.
- Para la característica de servidor de listas, se requiere Microsoft Message Queueing Services.

3.6.1.3 PRECIOS

Los precios incluye 3 meses de soporta gratis a partir de la compra y 1 año de actualizaciones antispam.

		Precio			Precio
10 buzones	ME10	$ 295	250 buzones	ME250	$ 950
25 buzones	ME25	$ 315	500 buzones	ME500	$ 1050
50 buzones	ME50	$ 495	Ilimitado buzones	MEUNL	$ 1250
100 buzones	ME100	$ 625			

Tabla 3.4 Lista de Precios de Antispam

[Texto tomado de : http://www.gfihispana.com/es/mes/]

3.6.2 SYMANTEC ANTISPAM™ PARA SMTP

3.6.2.1 CARACTERÍSTICAS PRINCIPALES

Proporciona protección completa contra los mensajes de spam en el gateway de correo electrónico de Internet.

Combina múltiples tecnologías de niveles basadas en la fuente de origen y en la detección de contenidos para controlar los mensajes de spam.
Incrementa la detección y reduce los falsos positivos utilizando una avanzada heurística de control de mensajes de spam, listas negras y listas blancas que reducen los gastos y el costo de la administración.

Ofrece administración remota, avanzadas funciones de alerta y gestión de informes a través de una interfase HTML intuitiva.

Prevención de múltiples niveles del spam Symantec AntiSpam para SMTP es una solución de control de mensajes de spam altamente integrada y de múltiples niveles que los detiene combinando enfoques, entre los que se incluye detección heurística y compatibilidad con múltiples servicios de lista negra en tiempo real. Otros niveles incluyen listas de bloqueo de remitentes personalizadas para bloquear por el primer y segundo nivel de dominio, y por direcciones de correo electrónico; y compatibilidad con listas blancas para corregir los falsos positivos y prevenir rápidamente. A través de su enfoque de prevención de spam de múltiples niveles, Symantec AntiSpam para SMTP

proporciona la flexibilidad para implementar eficazmente medidas de control a nivel del gateway.

Control del spam en el Gateway

Symantec AntiSpam™ para SMTP detiene los mensajes de spam en el primer punto de entrada de la red: el Gateway SMTP.

Además, al utilizar niveles de detección basados en fuentes de origen clave a nivel del Gateway, Symantec AntiSpam para SMTP minimiza el volumen general de mensajes de Spam que requieren revisión administrativa o del usuario final, así como su impacto en los servidores internos de mensajería.

Bloqueo por origen

Utilizando el bloqueo por fuente de origen, los administradores pueden minimizar los volúmenes de contenido no deseado en el primer punto de entrada sin necesidad de revisiones o procesos adicionales. Además de reducir significativamente el volumen de mensajes entrantes, esto también minimiza los gastos de administración. Para ello, Symantec AntiSpam para SMTP utiliza principalmente los siguientes dos métodos:

Listas negras personalizadas

Los mensajes de spam pueden bloquearse de forma flexible basándose en direcciones de correo electrónico plenamente calificadas, nombre del dominio o segundo nivel del dominio. También se admite el uso de comodines.

Compatible con múltiples listas negras en tiempo real

Un primer nivel eficaz contra los mensajes de spam son las listas negras basadas en DNSBL (en tiempo real), también conocidas como RBLs. Actualmente, existen más de 100 servicios de listas negras (RBL) en tiempo real en Internet. Como cada uno de los servicios de listas negras está basado en fuentes de spam diferentes, utilizar una combinación de las listas minimizará el número total de mensajes de spam procedentes de las distintas fuentes. Symantec AntiSpam para SMTP es compatible con cualquier servicio de lista negra conforme a DNSBL, así como con varios servicios simultáneamente.

Bloqueo por contenido

Al habilitar a los administradores para bloquear mensajes por el tipo de contenido, Symantec AntiSpam para SMTP ayuda a eliminar los mensajes de spam que pueden sobrecargar los recursos de servidor y el espacio de almacenamiento del correo y afectar la productividad del usuario final.

Avanzada heurística de control de los mensajes de spam

Uno de los niveles clave de la detección basada en contenidos es la heurística antispam de Symantec basada en tecnología de aprendizaje de las máquinas de redes neurales. El motor de heurística antispam está entrenado para distinguir tanto los mensajes comerciales de correo electrónico deseados de los no deseados, como los mensajes personales. Esto aumenta la efectividad y precisión de la solución para interceptar

mensajes de spam, especialmente si se le compara con las soluciones tradicionales basadas en palabras clave. Los mensajes que parecen spam se marcan para su futura revisión. Una vez marcados, estos mensajes pueden enviarse directamente de Symantec AntiSpam para SMTP a una casilla de correos de "cuarentena de spam" o pasarse al cliente de correo del usuario final donde se filtran a una carpeta de spam para su revisión periódica.

Bloqueo por línea Asunto

Symantec AntiSpam para SMTP también es compatible con el bloqueo de mensajes por línea Asunto para detener mensajes de spam con contenidos típicos, como "Viagra" o "Gane dinero". Para agregar mayor flexibilidad a la detección por la línea Asunto, también se admite el uso de comodines.

Prevención de falsos positivos

La prevención de mensajes de spam se ocupa no solo de la detección, sino también de la corrección e incluso en primer lugar, de la prevención de falsos positivos.

Listas blancas personalizadas

Symantec AntiSpam para SMTP permite a los administradores agregar fácilmente dominios "autorizados" a una lista blanca personalizada para permitir a los mensajes procedentes de dichos dominios evitar tanto las listas negras en tiempo real como los niveles de detección heurística antispam. Si ocurre que verdaderos boletines de noticias

voluminosos se marcan como spam, o si la organización tiene un servidor de correo en una lista negra, el agregar el dominio a la lista blanca permitirá que las próximas entregas lleguen a destino sin marcar. Además, al agregar pro activamente dominios de clientes y socios conocidos y de confianza, la solución no analizará los mensajes de correo procedentes de dichas fuentes, asegurando así la pronta entrega de las comunicaciones comerciales estándar, sin retrasos innecesarios.

Protección antispam independiente

Symantec AntiSpam para SMTP está basado en la solución de Gateway de SMTP de Symantec, Symantec Antivirus™ para SMTP Gateways, que incluye amplias capacidades de protección contra virus. En las organizaciones que ya cuentan con análisis de virus en el Gateway, Symantec AntiSpam para SMTP puede implantarse en el mismo servidor para permitir a los clientes la posibilidad de implementar medidas de control de mensajes de spam sin causar impacto en la infraestructura existente. Como retransmisor del filtrado de correo electrónico y gracias a su flexible enrutamiento y manejo de mensajes, Symantec AntiSpam para SMTP se integra sin obstáculos en su infraestructura de mensajería para agregar otro nivel de protección contra la amenaza que representan los mensajes de spam.

Fácil de administrar

Symantec AntiSpam para SMTP ofrece una interfase de usuario basada en HTML que permite administrar y configurar a distancia. La consola de administrador también

admite el acceso a múltiples niveles para permitir a los administradores de menor nivel realizar las tareas administrativas de rutina, al mismo tiempo que impide que modifiquen los parámetros de configuración críticos. El monitoreo del estado en tiempo real permite a los administradores actualizar las medidas de rendimiento de los servidores SMTP con un solo clic de botón que suministra el número de mensajes procesados, el número de mensajes en cola y muchas otras estadísticas en tiempo real. Su completo registro de actividades ayuda a los administradores a realizar un seguimiento de la actividad de spam, incluyendo las acciones de mensaje y sistema y exporta los archivos de registro en los formatos más populares de hoja de cálculo o base de datos. Sus flexibles funciones de información permiten a los administradores generar informes detallados y resumidos de la actividad de spam, a fin de permitir a las organizaciones analizar la actividad y evaluar la efectividad de su inversión en el control de mensajes de spam.

3.6.2.2 REQUERIMIENTOS TÉCNICOS

SOLARIS

- Servidor basado en SPARC
- Solaris 7 u 8
- 256 Mb de RAM como mínimo (512 Mb o superior recomendado para un rendimiento óptimo)
- 50 Mb para la instalación

- 500 Mb de espacio mínimo después de la instalación para procesamiento del correo
- Microsoft Internet Explorer 5.0 o superior o Netscape Navigator 4.7

WINDOWS® NT/2000 SERVER:

- Compatible con Intel® Pentium®
- Windows 2000 Server SP2 o Windows NT 4.0 SP3 o posterior
- 256 Mb de RAM como mínimo
- 50 Mb para la instalación
- 500 Mb de espacio mínimo después de la instalación para procesamiento del correo
- Microsoft Internet Explorer 5.0 o superior o Netscape Navigator 4.7

[Texto tomado de: http://enterprisesecurity.symantec.com/products]

3.6.3 SPAM ASSASSIN

SpamAssassin es una herramienta de reconocimiento automático de Spam. Analizando los correos que llegan a un usuario y siguiendo ciertas reglas decide cuáles tienen aspecto de Spam y actúa en consecuencia, típicamente marcándolos o etiquetándolos con la cadena en el asunto y explicando en el cuerpo por qué el correo recibido tiene

aspecto de Spam. El usuario puede actuar con los correos marcados como le parezca o por ejemplo eliminándolos.

Emplea desde reglas pre-configuradas de cabecera y contenido, hasta comprobaciones en los RBL, filtros bayesianos con autoaprendizaje, y puede interactuar con otras aplicaciones .

3.6.3.1 CARACTERÍSTICAS PRINCIPALES

SpamAssassin utiliza una amplia variedad de pruebas locales y de la red para identificar firmas del spam.

Software gratuito

Es distribuido gratuitamente bajo algunos términos y condiciones con otros software populares de código abierto como lo es Apache Web Server.

Fácil para Extenderse

Las pruebas Contra-Spam y la configuración se almacenan en texto llano, haciéndolo fácil configurar y agregar nuevas reglas.

Flexible

SpamAssassin encapsula su lógica en un API bien diseñado y abstracto así que puede ser integrado dondequiera en la corriente del correo electrónico. Las clases de

Mail::SpamAssassin se pueden utilizar en una variedad amplia de sistemas del correo electrónico incluyendo Procmail, Sendmail, posfijo, qmail, y muchos otros.

Fácil configuración

SpamAssassin requiere una configuración muy pequeña; No se necesita ponerlo al día continuamente con los detalles de sus cuentas del correo, cualidades de miembro de la lista a enviar, etc. Una vez que esté clasificado, el sitio y las políticas del usuario específicas éstas se pueden entonces aplicar contra el spam. Las políticas se pueden aplicar en ambos servidores del correo y más adelante usar el propio agente del correo del usuario.

Tecnología de filtrado Bayesiano

El filtro Bayesiano utiliza una aproximación matemática basada en el spam y el ham (correo válido) conocido. Esto le proporciona una tremenda ventaja sobre otras soluciones Antispam que sólo comprueban palabras clave o se fían de descargas de firmas de spam conocido. El filtro Bayesiano utiliza una fórmula matemática avanzada y un conjunto de datos que es creado personalizadamente para su instalación.

[Texto tomado de : http://spamassassin.apache.org/]

3.7 SOLUCIONES GATEWAY APPLIANCES

Ventajas adicionales

Estos equipos poseen las mismas ventajas que los mail Gateway mencionados anteriormente sumándose a estas las siguientes :

- Ofrecen una completa protección preventiva frente a amenazas provenientes del Internet ya que se pueden instalar detrás de cualquier Firewall protegiendo mi red interna.
- Plena cobertura de todos los protocolos principales: Tráfico SMTP, HTTP, FTP, POP3, IMAP4 y NNTP.
- Instalación sencilla ya que una vez configurado trabajan solos y no existe la necesidad de efectuar cambios a la red ni a los equipos clientes de mi red
- Son dispositivos escalables que permiten ir creciendo con forme las necesidades de la empresa.

Desventajas

- Costo elevado
- Originan cuellos de botella
- Son dispositivos con capacidad limitada de tráfico

3.7.1 PANDA GATEDEFENDER

Panda GateDefender es un appliance escalable y fiable que aporta la máxima protección en el principal punto de entrada a la red a través de su Hardware y Software de alto rendimiento, bloqueando virus, spam, contenidos no deseados y otras amenazas que puedan provenir de Internet antes de que entren en la empresa. Su sencillo manejo "conectar y olvidar" y completa protección antivirus, antispam y Filtrado Web, hacen de Panda GateDefender una potente solución de bajo coste de propiedad.

Panda GateDefender cuenta con un sistema de auto-actualización que verifica automáticamente la existencia de nuevas versiones del fichero de firmas convirtiéndose en la protección más actualizada de la empresa, con un funcionamiento óptimo y mínimo impacto en la velocidad de su red, siendo inapreciable para los usuarios de la misma.

Gracias a su balanceo de carga nativo se adapta a las necesidades de cualquier empresa, desde PYMEs a grandes empresas o ISPs ajustando su capacidad de análisis al tipo de tráfico y a las comunicaciones de la red. Existen tres modelos:

- Panda GateDefender 8050, hasta 25 usuarios; 120.000 mensajes por hora en tráfico SMTP; 5 Mbps en tráfico HTTP.
- Panda GateDefender 8100, de 25 a 500 usuarios; 300.000 mensajes por hora en tráfico SMTP; 14 Mbps en tráfico HTTP.

- Panda GateDefender 8200, a partir de 500 usuarios; 600.000 mensajes por hora en tráfico SMTP; 30 Mbps en tráfico HTTP.

3.7.1.1 CARACTERÍSTICAS PRINCIPALES

- Diseñado para ofrecer un alto rendimiento y capacidad de transferencia de sus motores de análisis, gracias a la integración de hardware y software.
- Posee un óptimo funcionamiento le permite tener un mínimo impacto sobre la carga de la red.
- Alta escalabilidad y balanceo de carga, aumentando su capacidad de análisis y transferencia en función del volumen de tráfico de la red.
- Gran sencillez en la instalación y configuración para facilitar su implementación y gestión.
- Protección para los protocolos de comunicación más usados: HTTP, FTP, SMTP, POP3, IMAP4 y NNTP.
- Filtrado de contenidos para el bloqueo de virus desconocidos y gusanos potencialmente peligrosos.
- Protección antispam, que reduce el impacto negativo de los correos no solicitados en su productividad.
- Filtrado web por categorías, que evita el acceso de los usuarios a contenidos no deseados.

- Administración remota y segura a través de consola web.
- Actualizaciones diarias y verdaderamente automáticas contra los nuevos virus.
- Informes detallados y alertas personalizables.
- Monitorización de sistemas en tiempo real.

3.7.1.2 REQUERIMIENTOS TECNICOS

Dispositivos Panda GateDefender 8085, 8100, 8200

[Texto tomado de : http://empresas.pandasoftware.es/productos/gatedefender/#e11]

3.7.2 WEBSHIELD 3000 SERIES APPLIANCES

Parte de la familia McAfee Secure Content Management, McAfee WebShield 3000 Appliances son soluciones para el Gateway de Internet y que exploran el tráfico de entrada y de salida en busca de protocolos SMTP, HTTP, FTP y POP3. Los dispositivos ofrecen un nivel inigualable de rendimiento y de capacidad de detección y limpieza de virus, así como de protección contra el correo no deseado de tipo spam y el contenido desechable, a empresas de cualquier tamaño.

3.7.2.1 CARACTERÍSTICAS PRINCIPALES

- Completa protección preventiva antivirus.
- Explora los principales protocolos de mensajería
- Fácil instalación
- Filtrado avanzado de contenido.
- Control basado en políticas mediante extended Policy Support
- Informes completos y análisis de tendencias y dispositivos múltiples
- Filtrado contra el robo de identidad
- Alto rendimiento, alta adaptabilidad

3.7.2.2 REQUERIMIENTOS TÉCNICOS

Dispositivos McAfee Webshield/SpamKiller 3100, 3200, 3300.

[Texto tomado de :

http://www.mcafeesecurity.com/es/products/mcafee/antivirus/email/category.htm]

4. SELECCIÓN DE LA MEJOR SOLUCION INFORMATICA EN BASE A COSTOS, RECURSOS DE HARDWARE Y EFECTIVIDAD.

Nuestra solución va enfocada para pequeñas empresas que no cuentan con un fuerte presupuesto en la parte de seguridad informática.

Por las características especiales de seguridad, versatilidad y costos que permite la plataforma en la que se basa ésta solución como lo es el sistema operativo Linux hemos seleccionado está solución como la adecuada.

4.1 VENTAJAS

Plataforma LINUX

La plataforma utilizada está evolucionando por ser una herramienta robusta, segura y económica.

Software antivirus de Calidad comprobada

Existe varias soluciones antivirus que funcionan bajo la plataforma de Linux. Sin embargo nosotros hemos escogido la proporcionada por Panda Labs ya que es la que presentamos como ejemplo en este trabajo de investigación.

El software Panda SendmailSecure ha sido evaluado y galardonado con las más altas distinciones como las obtenidas por West Coast Checkmark 100%, la certificación de ICSA Labs. Etc.

Costos Hardware

Los recursos de Hardware que esta solución necesita son muy económicos puesto que Linux funciona con mucha efectividad en un computador Pentium III de 200Mhz o superior con 64 MB de RAM como mínimo y 80 MB de espacio libre.

Un equipo con esas características o superior cuesta alrededor de $ 500

Costos de sistema operativo

Se debe tener instalada cualquiera de los siguientes Sistemas operativos Linux Red Hat(versiones 7.0 o superior), SuSE 7.3 o superior, Mandrake(versiones 8.0 o superior), o Debian 3.0 (Woody).

Costos software antivirus

El Panda SendmailSecure tiene un costo de $180 por servidor Gateway

4.2 DESVENTAJAS

Único motor antivirus

El software Panda posee un único motor antivirus en comparación a otros productos que poseen varios motores antivirus incluidos en él como un solo producto.

No se integra estrechamente con el sistema de Correo.

Ya que ésta solución funciona como Gateway en un equipo aparte. Esté software no posee las herramientas de integración con el software del servidor de correo.

Solo protege el correo externo y no la mensajería interna.

La protección es específicamente para la mensajería que proviene desde Internet vía SMTP ya que la mensajería interna que se produce dentro del sistema de mensajería de la empresa no es analizada.

5. DISEÑO E IMPLEMENTACIÓN DE EN UN MAIL GATEWAY ENTRE UN SERVIDOR DE CORREO BASADO EN TECNOLOGIA NOVELL GROUPWISE Y UN SERVIDOR BASADO EN LINUX SEDMAIL

Se ha implementado un diseño de protección de mail Gateway para un servidor Netware con sistema de mensajería Groupwise. La implementación está conformada por 3 servidores detallados a continuación.

5.1.1 ESPECIFICACIONES TÉCNICAS

Servidor Novell

- Procesador Pentium III 500 Mhz(o superior) con 512 MB de memoria RAM
- Sistema operativo Netware versión 5.5
- Sistema de correo con Groupwise versión 5.0 (o superior)

Servidor Gateway

- Procesador Pentium II 200 MHz (o superior), con 64MB de memoria RAM y 90MB de espacio libre en disco duro. Sistema operativo para

integración con AdminSecure o instalación independiente: Red Hat 7.0, 7.1, 7.2, 7.3, 8.0, 9.0 y Red Hat Enterprise, SUSE 7.3, 8.0, 8.2,9.0 ó 9.1 o Debian 3.0 (Woody).

- Otros sistemas operativos soportados para una instalación independiente: Red Hat 6.2 o Best Linux 2000.
- Servidor SMTP Sendmail versiones 8.11.3. o superior
- 2 tarjetas de red

Servidor Windows

- Procesador Pentium IV con 256 MB de memoria RAM
- Sistema operativo Windows 2000 Server
- Sistema de correo con Microsoft Exchange Server 2000

Software de protección Antivirus y AntiSpam

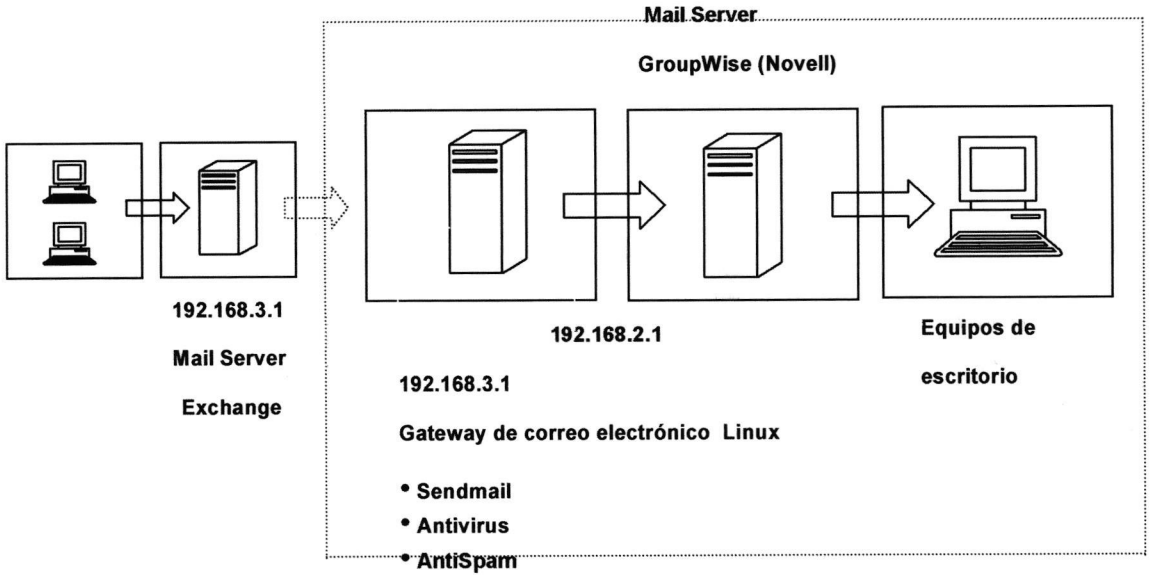
El software de protección instalado en el equipo Gateway es el Antivirus y Antispam SendmailSecure versión 1.62.

Los equipos se encuentran conectados a un dispositivo swich conformado 2 redes independientes. Cada una de estas redes con un dominio diferente cuyas direcciones IP se detallan a continuación:

Red	Servidor	Sistema de Mensjería	Dominio
192.168.2.0	Novell	Groupwise	A
192.168.3.0	Windows	Exchange	B

Los mensajes que son enviados al servidor Groupwise (Maneja dominio A) o que salen de ese servidor son filtrados por el Gateway de correo SMTP y analizados respectivamente. Los e-mail con problemas de virus o Spam son eliminados en este equipo por el software SendmailSecure y posteriormente este software envía un mensaje de alerta al administrador y al remitente. A continuación mostramos el diagrama de red en donde se detalla de mejor manera la implementación.

5.1.2 DIAGRAMA DE RED



CONCLUSIÓN Y RECOMENDACIONES

El uso intensivo de las telecomunicaciones por parte de las compañías para integrar sus procesos de negocio con sus socios, proveedores y clientes multiplica el riesgo de sufrir una infección de virus informáticos, por lo cual toda empresa por pequeña que sea debe tener protegido su sistema de mensajería.

La entrada de virus al sistema informático puede ocurrir por cualquiera de los siguientes puntos indicados a continuación:

- Periféricos de los ordenadores.
- Recursos compartidos en equipos conectados a redes de área local.
- Correo electrónico.
- Internet.

Dado que no existe la seguridad total, y ningún sistema antivirus nos ofrece una protección perfecta, siempre nos encontramos con debilidades y fortalezas que estos programas tienen, pero el uso correcto de estas herramientas produce una sensible reducción de los daños y pérdidas provocadas por este flagelo en la red. La selección

adecuada de aquellos productos que son fuertes en un determinado campo nos van a permitir tener una red menos propensa a ataques de virus.

Nuestra recomendación es que se debe tener cuidado con estos cuatro puntos, sin descuidar ninguno de ellos, saber seccionar aquellos productos antivirus y seguridad que nos ofrezcan un alto porcentaje de efectividad de detección de virus y de amenazas.

ANEXO - A

ORGANISMOS DE CERTIFICACIÓN DE SOFTWARE DE SEGURIDAD

CERTIFICACIÓN ICSA

Desde hace más de una década ICSA Labs, división independiente de TruSecure Corporation es una autoridad mundialmente reconocida para la certificación y testeo de productos de seguridad informática. ICSA Labs ha fijado estándares y certificado más del 90% de la base instalada de antivirus, firewalls, IPSec, criptografía y firewalls personales.

Además, ICSA Labs, publica encuestas, estudios de la industria de la seguridad informática y guías de productos a comprar.

Para todo producto de seguridad informática es un logro importantísimo, el contar con la certificación de ICSA Labs.

VIRUS BULLETIN 100%

Se otorga a los productos que detectan todos los virus "In the Wild" tanto en el escaneo bajo demanda (on-demand) como en

el escaneo en el acceso (on-Access) en los tests realizados por la publicación independiente **Virus Bulletin**.

Se introdujo en Enero del 98, y el logo incluye el mes en el que **Virus Bulletin** ha publicado los resultados de las pruebas, de modo que se pueden consultar en la Web de **Virus Bulletin** y constituyen una verdadera garantía de credibilidad.

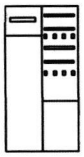
Los desarrolladores de Anti-Virus que puedan mantener sus soluciones más actualizadas, son los que podrán acceder más fácilmente a los premios **Virus Bulletin 100%**.

WEST COAST CHECKMARK 100%,

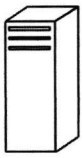
Las pruebas Checkmark han sido desarrolladas por los laboratorios West Coast Labs, centro independiente de investigación y pruebas de control, y proporcionan un marco de igualdad dentro del que se galardonan los productos que, de una manera consistente, ofrecen la máxima calidad entre las soluciones antivirus.

ANEXO - B

DISPOSITIVOS UTILIZADOS EN ESTE DOCUMENTO

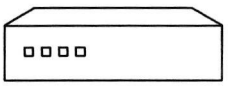


Representación de un Firewall



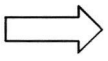
Representación de Servidor o Mail Gateway

Representación de un equipo de escritorio



Representación de Hub o Switch de comunicación

Representación de Internet



Representación de flujo de Correo Electrónico

BIBLIOGRAFIA

http://www.soho.com.mx

http://usuarios.lycos.es/nachos/2.html

http://usuarios.lycos.es/nachos/frames.html

http://www.europe.redhat.com/documentation/rhl9/rhl-rg-es-9/ch-email.php3

http://www.europe.redhat.com/documentation/rhl9/rhl-rg-es-9/s1-email-types.php3

http://usuarios.lycos.es/accimt/apuntes/si3.html

http://support.gfi.com/manuals/es/msec8/msec8manual_es-1-39.html

http://www.monografias.com/trabajos12/virudos/virudos.shtml

http://enciclopedia.us.es/index.php/Correo_basura

http://fmc.axarnet.es/redes/tema_04.htm

http://www.monografias.com/trabajos12/hisis/hisis.shtml#ma

http://usuarios.lycos.es/betzweb/

http://usuarios.lycos.es/mirella1324/newpage2.html

http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/SO14.htm

http://www.htmlweb.net/seguridad/varios/firma_certificados.html

http://www.ilustrados.com/publicaciones/EpyppFkVVEskVlMYZa.php

http://www.monografias.com/trabajos/soredes/soredes.shtml

http://www.isp2002.co.cl/virus.htm

http://www.gfihispana.com/es/mailsecurity/

http://enterprisesecurity.symantec.com/products

http://empresas.pandasoftware.es/productos/sendmailsecure/

http://www.gfihispana.com/es/mes/

http://empresas.pandasoftware.es/productos/gatedefender/#e11

http://www.mcafeesecurity.com/es/products/mcafee/antivirus/email/category.htm

http://support.microsoft.com/default.aspx?scid=kb;es;49500#kb1