

---

## **Proteger su red de las amenazas del correo**

---

La necesidad de una seguridad de correo integral basada en servidor

Este documento blanco explica por qué el software anti-virus no es suficiente para proteger a su organización de las actuales y futuras agresiones de virus y amenazas de correo. Examinando las diferentes clases de ataques por correo que amenazan a las organizaciones de hoy en día, este documento describe la necesidad de disponer de una sólida solución de seguridad de correo basada en servidor para salvaguardar su red.

---

## Introducción

Este documento blanco explica por qué el software anti-virus no es suficiente para proteger a su organización de las actuales y futuras agresiones de virus informáticos. Examinando las diferentes clases de amenazas de correo y métodos de ataque por correo, este documento describe la necesidad de disponer de una sólida pasarela de análisis de contenido basado en servidor para salvaguardar su negocio frente a los virus de correo electrónico y las agresiones, así como las pérdidas de información.

|   |   |
|---|---|
| Introducción .....  | 2 |
| La amenaza de los correos con virus y Troyanos.....                     | 2 |
| La amenaza de las fugas de información .....                            | 3 |
| La amenaza del correo con contenido malicioso u ofensivo .....          | 3 |
| Métodos usados para atacar su sistema de correo .....                   | 3 |
| La impresionante sencillez de crear un virus hoy .....                  | 5 |
| Por qué el software anti-virus o un cortafuegos no son suficientes..... | 5 |
| La solución: Una aproximación proactiva .....                           | 6 |
| Acerca de GFI MailSecurity for Exchange/SMTP .....                      | 6 |
| Acerca de GFI .....   | 7 |

---

## La amenaza de los correos con virus y Troyanos

El uso ampliamente generalizado del correo ha proporcionado a hackers y crackers una forma sencilla de distribuir el contenido dañino en la red interna. Los hackers pueden franquear fácilmente la protección ofrecida por un cortafuegos tunelizando mediante el protocolo de correo, ya que no analiza el contenido del correo.

CNN informó en Enero de 2004 que el virus MyDoom costó a las empresas unos 250 millones de US\$ en pérdida de productividad y gastos de soporte técnico, mientras NetworkWorld (Septiembre 2003) citaba estudios que situaban el coste de la lucha contra Blaster, SoBig.F, Wechia y otros virus de correo en 3.500 millones de US\$ sólo para las empresas norteamericanas.

Aún más, el correo también se utilizó para instalar Troyanos, diseñados específicamente para su organización, para obtener información confidencial o el control de sus servidores. Descritos como “virus instructivos” o “virus espía” por los expertos en seguridad informática, pueden ser potenciales herramientas de espionaje industrial. Un ejemplo claro es el ataque por correo sobre la red de Microsoft en Octubre de 2000, que un portavoz de Microsoft Corp. describió como "un auténtico acto de espionaje industrial". De acuerdo a los informes, la red de Microsoft fue asaltada mediante un virus Troyano *backdoor* enviado por correo a un usuario de la red.

---

## La amenaza de las fugas de información

Las organizaciones a menudo no reconocen que hay un gran riesgo de robo de datos cruciales en las empresas. Varios estudios han mostrado cómo los empleados utilizan el correo para enviar información empresarial confidencial. Ya sea porque estén descontentos y tengan deseos de venganza, o porque no se den cuenta del potencial impacto dañino de dicha práctica, los empleados utilizan el correo para compartir datos sensibles que fueron oficialmente recogidos para permanecer en la organización.

Como demostró la investigación Hutton 2003 en el Reino Unido, los empleados gubernamentales y los ejecutivos de la BBC han utilizado el correo para hacer revelaciones que eran confidenciales. Un artículo de PC Week en Marzo de 1999 se refería a un estudio en el que, de 800 trabajadores encuestados, entre el 21% y 31% admitieron haber enviado información confidencial por correo electrónico - como datos financieros o de producto - a destinatarios de fuera de la empresa.

---

## La amenaza del correo con contenido malicioso u ofensivo

El correo enviado por los empleados que contenga racismo, sexismo y otro material ofensivo puede hacer vulnerable a su empresa desde un punto de vista legal. En Septiembre de 2003, la firma Británica Holden Meehan Independent Financial Advisors tuvo que pagar £10.000 a un antiguo empleado por no protegerle del hostigamiento por correo. Chevron tuvo que pagar 2,2 millones de US\$ a cuatro empleados después de haber presuntamente recibido mensajes sexualmente ofensivos. Bajo la ley Británica, los empleadores son responsables del correo escrito por los empleados en el curso de su trabajo, independientemente de que el empleador consintiese dicho correo. La compañía de seguros Norwich Union fue requerida a pagar 450.000 US\$ en un acuerdo extrajudicial como resultado de comentarios sobre la competencia enviados por correo electrónico.

---

## Métodos usados para atacar su sistema de correo

Para enfrentarse con la clase de amenazas de correo presentes hoy, lo mejor es echar un rápido vistazo a los principales métodos actuales de ataque por correo. Estas incluyen:

### Adjuntos con contenido malicioso

Melissa y LoveLetter estuvieron entre los primeros virus en ilustrar el problema del correo con adjuntos y de confianza. Hacían uso de la confianza que existe entre amigos y compañeros. Imagine recibir un adjunto de un amigo que le pide que lo abra. Esto fue lo que ocurrió con Melissa, AnnaKournikova, SirCam y otros gusanos similares. Al funcionar, dichos gusanos suelen proceder a enviarse a si mismos a direcciones de correo de la libreta de direcciones de la víctima, de correos anteriores, de cachés de páginas web en el equipo local y métodos

similares. Los creadores de virus ponen mucho énfasis en conseguir que la víctima ejecute el adjunto. Por lo tanto hacen uso de atractivos nombres de archivo, como SexPic.cmd y me.pif.

Muchos usuarios intentan evitar la infección de virus de correo haciendo doble clic sólo en los archivos con ciertas extensiones, como JPG y MPG. Sin embargo, algunos virus, como el gusano AnnaKournikova, hacen uso de múltiples extensiones para intentar engañar al usuario y que abra el archivo. El virus AnnaKournikova fue transmitido mediante un adjunto llamado 'AnnaKournikova.jpg.vbs' que engañaba a los destinatarios haciéndoles creer que estaban recibiendo una inofensiva imagen JPG de la famosa estrella del tenis, en lugar de un Script de Visual Basic que contenía código infeccioso.

Además, la extensión Class ID (CLSID) permite a los hackers ocultar la extensión real del archivo, y en consecuencia el hecho de que cleanfile.jpg es realmente un feo archivo HTA (aplicación HTML).

Actualmente este método evita varias soluciones de filtrado de contenido de correo que hacen uso de métodos simples de comprobación de archivo, habilitando al hacker para llegar al usuario objetivo con mayor facilidad.

### **Correos que activan conocidas vulnerabilidades**

El gusano Nimda tomó Internet por sorpresa, evitando muchas herramientas de seguridad de red y asaltando servidores y redes empresariales así como infectando a usuarios domésticos. El truco de Nimda es que funciona automáticamente en equipos que tengan una versión vulnerable de Internet Explorer o Outlook Express. Nimda fue uno de los primeros de una línea de virus que aprovechan un defecto u otro para poder diseminarse. Variantes del virus Bagle que apareció en Marzo de 2004, por ejemplo, aprovechaban un antiguo defecto de Outlook con objeto de difundirse sin intervención del usuario.

### **Correo HTML con secuencias de comandos incrustadas**

Actualmente, todos los clients de correo pueden enviar y recibir correo HTML. El correo HTML puede incluir scripts y Contenido Activo que puede permitir que programas o código se ejecuten en el equipo cliente. Outlook y otros productos utilizan componentes de Internet Explorer para mostrar correo HTML, lo que significa que heredan las vulnerabilidades de seguridad encontradas en Internet Explorer.

Los virus basados en secuencias de comando HTML tiene el peligro añadido de ser capaces de iniciarse automáticamente cuando se abre el correo malicioso. No confían en los adjuntos; por lo tanto filtros de adjuntos de las aplicaciones anti-virus no son de utilidad para combatir los virus con secuencias de comandos HTML desconocidas.

El virus BadTrans.B, por ejemplo, combina una vulnerabilidad de correo con HTML para propagarse, utilizando HTML para lanzar un adjunto automáticamente una vez se recibe el

correo.

---

## **La impresionante sencillez de crear un virus hoy**

Cualquiera con un poco de conocimiento de Visual Basic puede desatar el caos mediante el aprovechamiento de vulnerabilidades bien conocidas de varios clientes de correo y productos comúnmente utilizados. Una visita al sitio SecurityFocus, por ejemplo, revelará varias vulnerabilidades que están disponibles en Microsoft Outlook. Un novato de las secuencias de comandos maliciosos con la intención de producir un virus puede simplemente modificar el código de vulnerabilidad - ¡que está públicamente disponible! – para ejecutar su código.

Por ejemplo, una vulnerabilidad de Internet Explorer y MS Access, que podría ser fácilmente aplicada a Outlook y Outlook Express, se describe en Guninski.com. Una creador de virus podría fácilmente aprovecharlo para ejecutar código Visual Basic en el momento en que la víctima abra el correo infectado. Esto infectaría todos los archivos HTML y se enviaría a sí mismo a todos los contactos de la libreta de direcciones del destinatario. Una característica clave de este virus, sin embargo, es que se ejecutaría simplemente cuando el usuario abriese el correo que contiene HTML malicioso.

---

## **Por qué el software anti-virus o un cortafuegos no son suficientes**

Algunas organizaciones confían demasiado en si mismas tras la instalación de un cortafuegos. Este es uno de los pasos para proteger su intranet, pero no es suficiente: Los cortafuegos pueden prevenir el acceso a su red por usuarios no autorizados. Pero no comprueban el contenido del correo enviado y recibido por aquellos autorizados para utilizar el sistema, por ejemplo. Esto significa que el correo con virus aún pasa a través de este nivel de seguridad.

Y tampoco el software de análisis anti-virus protege contra TODOS los virus y ataques de correo: Los fabricantes de anti-virus no siempre pueden actualizar sus firmas a tiempo contra los mortales virus que se distribuyen por todo el mundo mediante el correo en cuestión de horas (como los recientes gusanos MyDoom, NetSky.B y Beagle). Las empresas que utilizan un único motor anti-virus no están necesariamente salvaguardadas cuando aparece un nuevo virus. Un estudio de 2004 del gobierno del Reino Unido encontró, por ejemplo, que aunque el 99% de las grandes empresas Británicas utilizan productos anti-virus, el 68% de ellas fueron infectadas por virus durante el 2003. Similarmente, un estudio de 2003 llevado a cabo por los laboratorios de investigación de Hewlett-Packard en Bristol, encontró que el método de actualizar las firmas para la detección y eliminación de virus es fundamentalmente defectuoso, simplemente porque los gusanos pueden difundirse más rápido que la distribución de actualizaciones de firmas anti-virus.

---

## **La solución: Una aproximación proactiva**

Pero entonces, ¿cómo se protege uno de las amenazas de correo? Es necesaria una aproximación proactiva que implique el análisis de contenido de todo el correo entrante y saliente a nivel de servidor, antes de la entrega a sus usuarios. De esta forma, todo contenido potencialmente nocivo es eliminado del correo infectado o dudoso, y sólo entonces es entregado al usuario.

Mediante la instalación de una pasarela de análisis de contenido del correo y anti-virus en su servidor de correo, las empresas pueden protegerse contra los daños potenciales y contra la pérdida de tiempo laboral que puedan causarles actuales y futuros virus.

---

## **Acerca de GFI MailSecurity for Exchange/SMTP**

GFI MailSecurity for Exchange/SMTP es una solución de análisis de contenido, detección de debilidades, análisis de amenazas y anti-virus para el correo que elimina todo tipo de amenazas de correo antes de que puedan afectar a los usuarios de una organización. Las características clave de GFI MailSecurity incluyen múltiples motores anti-virus, para garantizar un ratio de detección más alto y una respuesta más rápida a los nuevos virus; análisis de contenido y adjuntos, para poner en cuarentena adjuntos y contenido peligroso; una pantalla frente a debilidades, para protegerse de virus presentes y futuros que se basan en vulnerabilidades; un motor de amenazas HTML, para desactivar los scripts HTML; y un Escáner de Troyanos y Ejecutables, para detectar ejecutables maliciosos. Para leer más y descargar una versión de evaluación, visite <http://www.gfi.com/mailsecurity/>.

---

## Acerca de GFI

GFI es un destacado desarrollador de software que proporciona una única fuente para que los administradores de red dirijan sus necesidades en seguridad de red, seguridad de contenido y mensajería. Con una galardonada tecnología, una agresiva estrategia de precios y un fuerte enfoque en las pequeñas y medianas empresas, GFI es capaz de satisfacer la necesidad de continuidad y productividad de los negocios que tienen las organizaciones en una escala global. Fundada en 1992, GFI tiene oficinas en Malta, Londres, Raleigh, Hong Kong, Adelaide y Hamburgo que soportan más de 200.000 instalaciones en todo el mundo. GFI es una empresa enfocada a canal con más de 10.000 partners en todo el mundo. GFI es también Microsoft Gold Certified Partner. Se puede encontrar más información sobre GFI en <http://www.gfihispana.com>.

© 2007 GFI Software. Todos los derechos reservados. La información contenida en este documento representa la visión del momento de GFI sobre lo discutido a la fecha de la publicación. Como GFI debe responder a las condiciones de los cambios del mercado, no debe ser interpretado como obligación por parte de GFI, y GFI no puede garantizar la exactitud de la información presentada después de la fecha de publicación. Este Documento Blanco solo tiene propósito informativo. GFI NO DA GARANTIA, EXPRESA O IMPLICITAMENTE, EN ESTE DOCUMENTO. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor y sus logotipos son marcas registradas o marcas de GFI Software en los Estados Unidos y/o otros países. Todos los nombres de producto o empresas mencionados pueden ser marcas registradas de sus respectivos propietarios.

