



Amenazas emergentes en la seguridad de las empresas

Hoy más que nunca, las empresas necesitan cuidar la seguridad de sus redes. El número, variedad y virulencia de las amenazas de seguridad en equipos y redes se ha incrementado dramáticamente, cambiando las necesidades de las empresas a la hora de prepararse contra ataques de *malware* en continua evolución que ya puede vislumbrarse en el horizonte.

Mientras la mayoría de fabricantes de seguridad tradicionales están focalizados en la protección de las aplicaciones de los equipos, ciertamente de carácter fundamental, las amenazas actuales más importantes - así como las emergentes más destacadas - son aquellas que se derivan de los nuevos estilos de vida online. Debido al importante incremento de los conocimientos informáticos y a la línea divisoria, cada vez más difusa, entre la actividad profesional y privada que se realiza en equipos y redes en las empresas, éstas necesitan tener un mayor cuidado del uso que sus trabajadores hacen de la red y asegurarse de que su seguridad informática no es un escollo.

Amenazas en el entorno empresarial – Dispositivos móviles, el último objetivo de los ataques

En 2007, el *malware* se convirtió en una de las principales amenazas para la seguridad de las redes. El *malware* está en continuo flujo y las únicas amenazas perceptibles en la actualidad son aquellas variantes de *malware* ya existentes, cada vez más sigilosas y orientadas a ataques focalizados.

Existen numerosos y documentados casos de recientes ataques de *malware* orientados hacia empresas (por ejemplo, utilizando archivos infectados de MS Office). En cada caso, el *malware* utilizado fue creado específicamente para la ocasión y pudieron verse pequeñas propagaciones más allá de las empresas inicialmente afectadas. Ante estos ataques sorpresa, las empresas deberían ponerse en guardia, especialmente teniendo en cuenta que el *malware* se vuelve cada vez más sofisticado y continúa atacando allí donde las empresas creían sentirse a salvo.

Los dispositivos móviles son una de las áreas donde han crecido significativamente los ataques de *malware*. Los usuarios de las tecnologías Smartphone han jugado un papel primordial en la transición de amenazas desde los equipos portátiles o *laptop* a dispositivos de mano tipo PDA. La reciente tendencia de incluir exploradores de Internet en dispositivos móviles y tener siempre disponible el acceso a Internet, ha volcado las amenazas de la red al mundo de la telefonía móvil y, por extensión, a todas aquellas empresas que se valen de estas nuevas tecnologías. Los virus que se aprovechan de las vulnerabilidades de los exploradores se convertirán en algo común.



A medida que se van añadiendo nuevas funcionalidades, la seguridad queda relegada a favor de la funcionalidad, dando origen a todo tipo de nuevas oportunidades para los ataques maliciosos. Como sucede con la mayoría de los virus en los PCs, el *malware* dirigido a los dispositivos móviles supondrá la eliminación de archivos, el envío de información privada facilitando ataques externos o harán que se agote la batería del dispositivo.

Las organizaciones deberían ser conscientes de la necesidad de proteger los dispositivos móviles de sus empleados de ataques de *malware*, ya que podría afectar gravemente la seguridad de sus redes.

La mejor defensa empresarial contra el *Malware*

Se suele decir que “más vale prevenir que curar”. Esta frase popular puede aplicarse hoy en día a las empresas: la mejor defensa es una buena protección. Una política de seguridad severa junto con el uso de soluciones de protección adecuadas minimiza el riesgo para las redes empresariales.

El antivirus es una herramienta de seguridad, pero no deja de ser una de las más importantes. Cada día, millones de ordenadores se infectan con virus, gusanos, troyanos y otras amenazas informáticas. Se ha contabilizado un promedio de un virus por hora.

A la hora de elegir el antivirus apropiado para cada red, es muy importante tener en cuenta la frecuencia de las actualizaciones. Si cada hora aparece un virus, la empresa no puede tener un antivirus que se actualice solamente una vez al día, o incluso con menos frecuencia, ya que se encontraría en una situación de vulnerabilidad a las nuevas amenazas durante al menos 24 horas. Ante la rapidez con la que se crean nuevas amenazas las compañías antivirus, conscientes de la importancia de la seguridad de sus usuarios, responden creando nuevas tecnologías de detección de amenazas basadas en el análisis del comportamiento. Estas tecnologías, denominadas heurísticas, han hecho posible la detección de virus y otro tipo de *malware* sin necesidad de analizar muestras en laboratorios antivirus, minimizando así el tiempo de respuesta ante las nuevas amenazas.

Una buena tecnología de detección heurística y la frecuencia de las actualizaciones marcan la diferencia entre los programas antivirus y la seguridad que estos pueden ofrecer.

Es también muy importante la educación del usuario. En una red en la que cada usuario sabe cómo evitar los ataques maliciosos, hay muchos menos problemas relacionados con la seguridad. No obstante, esta es la tarea más difícil de realizar. Mediante charlas de seguridad realizadas periódicamente se puede explicar a los empleados por qué no tienen que abrir un mensaje que llega desde un remitente desconocido, o por qué no tienen que descargar archivos desde Internet si no tienen programas antivirus instalados que puedan detectar si los archivos son realmente legítimos o están infectados.



Actualmente se están usando todos los medios para transmitir estos mensajes a los usuarios, pero pasará mucho tiempo hasta que todos sean conscientes de la importancia que tienen estos pequeños consejos en la seguridad de nuestros datos. Hasta que llegue ese momento, se recomienda usar el principio del mínimo privilegio, es decir, dar a los usuarios sólo los permisos que son necesarios para el desarrollo de su trabajo, asegurarse de que no pueden instalar aplicaciones maliciosas, y de que no pueden compartir archivos infectados con otros usuarios de la red. Los perfiles de los usuarios, donde se guardan los datos de éstos, deben almacenarse en servidores protegidos para así evitar la propagación en la red de archivos infectados.

Otras amenazas en el entorno empresarial

El *Spyware* sigue siendo una de las amenazas en continuo crecimiento para el sector empresarial. A la vista de la última legislación de protección de datos en Europa y Estados Unidos, el peligro para las empresas en términos de responsabilidad de la pérdida o robo de datos seguirá incrementándose en un futuro inmediato.

Las diferentes variantes del gusano "Storm Worm" todavía son una de las principales amenazas desde comienzos del 2008, al igual que la familia de troyanos "Trojan Zlob" que está en un continuo crecimiento y podría convertirse en una de las mayores amenazas de este año. Otro tipo de troyanos, dedicados a crear redes de ordenadores infectados para difundir virus, spam o para llevar a cabo prohibiciones de accesos a servicios, podrían destacar en los próximos meses.

Para las empresas, el uso de un buen Cortafuego sigue siendo un pilar fundamental para la seguridad de sus redes, especialmente a la hora de encargarse de amenazas automatizadas como gusanos o botnets (Redes Zombie), combinado con una potente protección antivirus tanto en los servidores, como a nivel de los clientes.

Los virus mensajeros masivos estuvieron bastante presentes en la primera mitad del 2007, pero existen otros tipos de amenazas que están tomando mayor relevancia, aunque el correo electrónico sigue siendo el medio preferido de muchos de estos ataques.

El uso de *adware* parece aumentar, a medida que se reduce el peligro legal para sus creadores. La pérdida de productividad de una empresa generada por la limpieza de equipos infectados es considerable, por lo que éstas deberían considerar la implementación de filtros web para prevenir la infección de este u otro tipo de *malware*.

El intercambio de archivos P2P se ha convertido en algo frecuente; el número, diversidad e impacto de archivos infecciosos ha crecido significativamente en el año anterior. EL trabajo de deshabilitar o limitar el tráfico P2P y otros métodos de intercambio de archivos puede, sin embargo, acarrear una serie de costes de productividad. En estos casos, es altamente recomendable instalar una solución antivirus en cada equipo así como en los servidores de ficheros.



El Spam se está diversificando y evolucionando con el objetivo de eludir los nuevos filtros, a través de constantes variaciones con una gran ofuscación tanto en contenido como en objetivos. El spam adjunto, aunque ha seguido una tendencia a la baja en los últimos meses del 2007, parece volver a aumentar y posiblemente sea algo a tener en cuenta de nuevo en este 2008. Las pérdidas de productividad procedentes del spam no son pocas. Las empresas en expansión deberían considerar la introducción de buenos filtros antispam tanto en servidores como en clientes.

Para conseguir una detección más fiable, existen nuevas técnicas alternativas al filtro OCR, dedicado a descifrar el texto que contienen las imágenes del spam. Una de las tecnologías más efectivas para la lucha del spam con imágenes se denomina SID, un filtro que ignora el texto dentro de las imágenes y que aprende de la experiencia de algunas características comunes de las imágenes. Este algoritmo selecciona las imágenes basándose en la similitud de los colores, en lugar de buscar la similitud en las formas y obtiene un ratio de detección del 98,7% de imagen del spam.

Otra de las nuevas tecnologías que está ofreciendo muy buenos resultados es la denominada NeuNet o red neuronal artificial. Esta red crea un proceso automático que reúne el 'spam' y el 'ham' (correo legítimo) durante un período de tiempo, estudiando sus características y aprendiendo de forma inteligente, sin necesidad de la intermediación de un ser humano.

La combinación de estos nuevos sistemas de detección junto con los algoritmos convencionales ofrecen una máxima efectividad en la lucha contra el spam, y permiten reconocer nuevas oleadas de correo basura con gran celeridad, algo primordial para la productividad de una empresa.

El *Phishing*, vía web y/o email, es probablemente la peor amenaza actual y continuará siéndolo durante el próximo año. También es una de las más peligrosas ya que causa pérdidas económicas directas al usuario a través del robo de información de cuentas bancarias que hacen que puedan quedar "limpias" en cuestión de días o incluso horas. El modo de operar más habitual en este tipo de spam es pedir al usuario que introduzca datos críticos como su número de cuenta y contraseña para "actualizar e incrementar" el grado de seguridad de su cuenta o "evitar su cancelación". Las plantillas utilizadas para crear este tipo de emails están cuidadosamente elaboradas y son extremadamente similares al diseño de las entidades bancarias, aunque en muchos casos las faltas de ortografía y una dirección web distinta a la original suelen delatarlos.