¿Su negocio está protegido?

Federico Chaniz
Manager Regional de
Blue Coat System

El software antivirus y los firewall son buenas soluciones para la seguridad de redes, pero llevan a las empresas a una falsa sensación de seguridad cuando se trata de amenazas basadas en la Web. Para poder combatir con éxito este nuevo tipo de infecciones, las Pymes requieren una herramienta de seguridad diseñada especialmente para la Web y las Redes Sociales.

El auge de Internet significó un gran impulso para las pequeñas y medianas empresas (Pymes) que, al igual que las empresas más grandes, continúan adoptando aplicaciones basadas en la Web y utilizan las redes sociales para conectarse con sus clientes, crear comunidades de clientes y de socios, así como también de productos y servicios de mercado, reclutar nuevos talentos y mucho más.

Desgraciadamente, los ciberdelincuentes también utilizan la web con otros fines, como el robo de identidad, el fraude, la propagación de malware y otros contenidos maliciosos. En consecuencia más de un millón de sitios son infectados con malware cada trimestre, incluyendo sitios de confianza, y hasta una de cada diez páginas Web, sin saberlo, podrían contener malware, según investigadores de la industria de seguridad.

La ciberdelincuencia también está contaminando los resultados de motores de búsqueda para dirigir a los usuarios desprevenidos hacia el malware. Los empleados remotos y móviles son aquellos mayormente expuestos, ya que pueden navegar por la Web sin protección y llevar malware a la red de la empresa cuando regresan a la oficina.

Para luchar contra esta nueva clase de amenazas, las Pymes necesitan una herramienta de seguridad hecha específicamente para la Web y las redes sociales.

Evitar una falsa sensación de seguridad

Muchas Pymes instalaron prudentemente software anti-virus (AV) en las computadoras de los empleados y/o desplegaron un firewall y/o una Gestión Unificada de Amenazas (UTM) en la red. Sin embargo, estas herramientas no fueron diseñadas para entender el contenido Web y no son eficaces contra las amenazas Web multi-dimensionales y altamente dinámicas de hoy, dando a las Pymes una falsa sensación de seguridad que las hace vulnerables.

Muchos sitios Web legítimos extraen contenidos de múltiples fuentes, como las redes de anuncios, noticias, videos y enlaces de referencia hacia otros contenidos, lo cual los convierte en buenos targets para sufrir los ataques de malware. Gracias al hackeo de un sitio Web conocido y de confianza, los criminales cibernéticos pueden aprovecharse de la buena reputación de la página Web para evitar ser detectados. Por ejemplo, en uno de los ataques más comunes en 2010, los servidores de anuncios fueron engañados ofreciendo anuncios que entregan software malicioso a los usuarios desprevenidos, incluso sin que los usuarios deban hacer clic en un enlace. Para evitar ser detectados, estos ataques basados en la Web son a menudo de corta duración, subsisten sólo unas horas, durante las cuales la ubicación del malware puede cambiar varias veces. En un ataque reciente, la ubicación del malware cambió más de 1.500 veces en un solo día.

Las defensas tradicionales, tales como software antivirus de escritorio, confían en el proveedor de seguridad para analizar una amenaza, identificar su firma y actualizar el software del cliente para bloquear esa firma. Este análisis se lleva a cabo después de que el ataque se ha puesto en marcha y puede tomar algunas horas o incluso días, tiempo durante el cual los clientes no están protegidos. Por su parte, firewall y plataformas UTM están diseñados para bloquear el tráfico basado en direcciones y números de puerto.

Si bien ambos son capas esenciales de una sólida estrategia de seguridad de red, ya no pueden proporcionar una defensa efectiva contra la nueva clase de amenazas dinámicas basadas en la Web. Las amenazas de seguridad basadas en la Web actuales provienen de contenidos Web, direcciones URL y active scripts. Los productos tradicionales de seguridad, o bien no pueden descifrar la información relacionada con la Web o lo hacen de manera limitada y estática. Teniendo en cuenta que el 50% de las medianas empresas reportaron infecciones por malware en 2010, las Pymes necesitan una solución de seguridad basada en la Web en tiempo real, además de AV y otros mecanismos de seguridad tradicionales.

La solución de seguridad ideal para la Web

Comprendiendo la naturaleza altamente dinámica de las amenazas basadas en la Web, es clave seleccionar el producto de seguridad adecuado.

Para lograr una solución integral de seguridad basada en Web para Pymes, que sea eficaz, deben considerarse los siguientes puntos:

- Una aplicación especialmente diseñada que bloquee el malware basado en la Web antes de que ingrese en la red de la empresa;
- Protección de los empleados remotos y móviles
- Un componente basado en la nube,

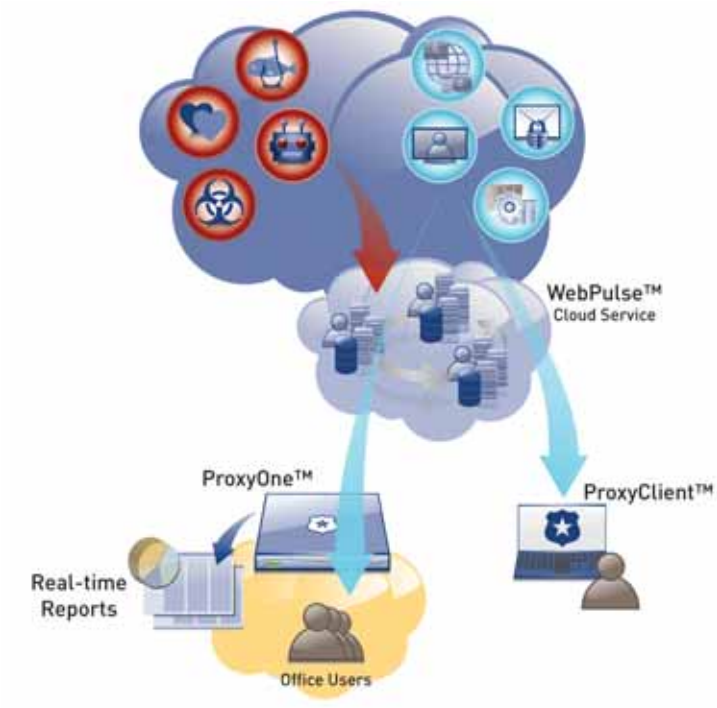
Continúa en página 184

que opere en tiempo real para analizar nuevas direcciones URL no reconocidas y contenido Web proveniente de una gran comunidad de usuarios y también para hacer que esos resultados estén de inmediato a disposición de los mismos.

Un dispositivo de seguridad web online actúa como una primera línea de defensa, chequea cada dirección URL, scripts y direcciones IP con la base de datos de amenazas conocidas y automáticamente bloquea a los usuarios las conexiones a sitios de malware conocidos. Dado que muchas de las amenazas basadas en la Web aparecen y desaparecen en cuestión de horas, es crucial que una solución de seguridad Web también provea un análisis dinámico de los nuevos sitios Web y contenidos, así como los usuarios se encuentren con éstos. La mejor manera de controlar la distribución de amenazas en tiempo real es mediante el uso de lo que la firma de investigación Enterprise Strategy Group llama "seguridad de la comunidad basada en la nube".

Con este enfoque, una gran comunidad de participantes obtienen beneficios de la inteligencia compartida acerca de las nuevas amenazas. URL desconocidas, active scripts, direcciones IP, y contenidos Web solicitados por miembros de la comunidad son pasados al proveedor de la nube de seguridad para su análisis.

El hecho de que la inteligencia basada en la nube debe estar inmediatamente disponible para todos los usuarios, incluidos los que son remotos o móviles, les garantiza a estos usuarios obtener la misma protección dinámica que aquellos ubicados dentro de la oficina.



El volumen de malware basado en Web, sin dudas, seguirá aumentando en los próximos meses. Las Pymes pueden estar seguras de que no serán tomadas por sorpresa con una nueva defensa que incluya una solución de seguridad dinámica específicamente diseñada para combatir las amenazas basadas en Web en tiempo real.

Acerca de Blue Coat

Blue Coat es líder tecnológico en Application Networking, ofreciendo una estructura que proporciona la visibilidad, aceleración y seguridad que se requieren para optimizar y asegurar el flujo de información a cualquier usuario, sobre cualquier red, en cualquier lugar. Esto permite a las empresas alinear sus inversiones en redes con los requisitos del negocio, agilizando la toma de decisiones ■

Más información: Zen Consulting - (54 11) 5218- 4845 - info@zenconsulting.com.ar - www.zenconsulting.com.ar

Blue Coat