

**Como el uso de Internet puede
poner en peligro su negocio.**

Introducción

Las pequeñas y medianas empresas confían en Internet como parte esencial de sus operaciones diarias. Ya que Internet ofrece rápido acceso a la información y permite comunicarse con el mundo exterior las 24 horas del día y los 7 días de la semana. Pero a pesar de estos magníficos beneficios, Internet inevitablemente pone a las empresas a merced de una gran variedad de amenazas contra la seguridad. Con sólo utilizar la navegación Web las empresas corren el riesgo de sufrir amenazas basadas en Internet, que se van multiplicando a medida que la actividad online se incrementa.

El Uso Inapropiado

Las empresas que fracasan filtrando o controlando el uso de Internet de sus empleados, ponen en riesgo la productividad de su equipo de trabajo, su reputación y la seguridad de su red informática. Los empleados suelen pasar una gran parte del tiempo navegando por Internet por motivos personales y profesionales. Muchos de ellos visitarán una tienda online, sitios peer-to-peer, y páginas de redes sociales, incluso páginas de citas o de adultos. Todas estas actividades hacen perder el tiempo a la empresa y además exponen la red informática a amenazas basadas en Internet.

Por ejemplo, las páginas para adultos son sumamente conocidas por alojar programas malignos. Estas páginas son fáciles y baratas de lanzar, contienen contenidos que atraen a muchos visitantes y son lo suficientemente tabú como para hacer que sus visitantes guarden silencio cuando sospechen que por su culpa se ha infectado su sistema. Estos atributos hacen de estas páginas el medio ideal para la propagación de programas malignos.

Las páginas de compra online son igualmente conocidas por alojar amenazas basadas en Internet. Los software espía proliferan en este tipo de páginas. Además estas páginas suelen tener un acceso a páginas de terceros para muchos de sus elementos, de forma completamente transparente para el usuario. Por ello, incluso cuando la página principal sea legal, el usuario raramente se da cuenta de cuando está en la página limpia o cuando en una página de terceros desconocida.

En una encuesta anual sobre brechas en la seguridad, dirigida por PricewaterhouseCoopers en nombre del BERR (Business Enterprise & Regulatory Reform) del Reino Unido, se descubrió que el año pasado una de cada seis empresas experimentó un mal uso de sus sistemas informáticos. De los casos reportados, el 36 por ciento pasaban demasiado tiempo navegando por Internet, y un 41 por ciento adicional accedía a páginas Web inapropiadas. Aunque menos frecuente, también había empleados que accedían a contenido ilegal.

La mayoría de este uso inapropiado, incluido la conducta cuestionable o peligrosa, se puede atribuir a la actitud despreocupada de la mayoría de los empleados tienen hacia sus equipos. Muchos empleados usan Internet pensando en que como no son sus ordenadores, la seguridad no es importante. De igual modo, muchos usuarios asumen que la seguridad es responsabilidad de los departamentos informáticos y consideran que su conducta peligrosa no debería tener un impacto negativo.

Vehículo de Amenazas Externas

Incluso cuando los empleados de las empresas utilizan Internet de forma apropiada, Internet sigue siendo la fuente principal de amenazas informáticas, como software espía, troyanos, bots, backdoors y rootkits. En muchos casos, la única interacción que se necesita para infectar el sistema es simplemente visitar una página web. Esta forma de transmisión se llama "drive-by download", que tiene lugar por detrás mientras el usuario realiza un uso normal de sus actividades online, sin el conocimiento ni la interacción del usuario.

De acuerdo al estudio ProSecure de NETGEAR, el 79 por ciento de estas amenazas se han descubierto en páginas legales que han sido pirateadas por hackers que han entrado a hurtadillas para infectar la página. En estos ataques, los las páginas que no hayan instalado los parches de seguridad adecuados. Como resultado cualquier página puede infectarse. En los primeros 4 meses del año 2008, centenares de páginas que pertenecían a Fortune 500, empresas, agencias gubernamentales y escuelas informaron que habían sido infectadas por código maligno. Incluso conocidas empresas de seguridad como Symantec, Trend Micro y Computer Associates tenían sus páginas Web comprometidas.

Los agresores han aprendido a utilizar páginas legales como cebo para tácticas de "ingeniería social" que tentaba a los usuarios para que hiciesen click en un link incluido o en el adjunto del e-mail. En Diciembre del 2008, la popular red social "Facebook" se utilizó para un ataque. Los usuarios recibían un e-mail con el título "Estás gracioso en este nuevo vídeo". En el mail se alentaba a los usuarios a pinchar en el link incluido para visualizar el vídeo. El link te llevaba a una página Web de vídeos que no pertenecía a Facebook e informaba al usuario de que se necesitaba una nueva versión del Flash Player para visualizarlo. Utilizando el link que ofrecía para hacerlo se instalaba un gusano en el sistema del usuario. El gusano incluía un software espía y abría una puerta trasera que permitía enviar información privada así como instalar más código en el futuro.

El 21 por ciento restante es el resultado de usuarios que visitan páginas maliciosas sin querer. Estas páginas se diseñan para parecer legítimas y atraer expresamente a usuarios confiados. Muchas de ellas utilizan incluso motores de búsqueda y anuncios en banners para aumentar el número de visitantes.

Drive-By Downloads

Un "drive-by-download" es una amenaza alojada en una página Web. Es un poco diferente a las otras amenazas comentadas. En este caso se confía en que la víctima vaya a la página en vez de que la amenaza sea enviada al sistema de la víctima. En un "drive-by-download" las amenazas tipo software espía, adware o troyanos se instalan sin el conocimiento o la interacción por parte del usuario. Cuando un usuario visita una página infectada la amenaza se descarga por detrás de forma automática. La página infectada puede ser una página corrupta desarrollada por un autor malicioso para parecer legítima o puede ser una página legítima pirateada e infectada por un autor malicioso. En cualquier caso, el usuario normalmente ni se entera de que se ha infectado.

Mediante la implantación de amenazas en páginas legítimas los atacantes obtienen visitantes. Desarrollando sus propias páginas corruptas, tienen más control sobre la amenaza. En cualquier caso parece aparente que bloquear las páginas basándose en sus contenidos ya no es lo adecuado para proteger la empresa de tales amenazas.

Protegiendo su Empresa

Los atacantes ven el sistema del usuario como el último obstáculo para llegar al objetivo real, la red de la empresa. Así que muchas amenazas entran a la red a través del sistema del usuario y entonces se propaga libremente. Una vez dentro estas amenazas pueden consumir grandes volúmenes del ancho de banda de la red, robar información privada de la empresa o de los clientes, dañar los ficheros del sistema o piratear los recursos de la empresa para lanzar spam y cualquier otra amenaza vía e-mail.

Así que como primera medida de defensa contra amenazas basadas en Internet se deben establecer y respetar unas reglas de Internet aceptables. Estas reglas deben incluir el tipo de páginas Web que pueden y no pueden ser visitadas, así como estimar una cantidad de tiempo aceptable. Sin embargo muchas empresas permiten a una parte su personal utilizar el equipo de la empresa para realizar actividad Web y ofrece a los empleados demasiada libertad lo que pone en peligro la empresa. Estas reglas no deben abarcar sólo la cantidad de tiempo que utilizarán los empleados para sus temas personales en Internet, sino también el tipo de páginas Web que se permitirá visitar.

Además de unas reglas de uso es esencial que la empresa instale un potente Gateway de Seguridad que incluya filtrado del contenido de las URL y control del tráfico bi-direccional. Mediante el filtrado del contenido de la URL el dispositivo de seguridad refuerza las reglas de la empresa bloqueando las URLs prohibidas y con contenido inapropiado. Cuando los empleados intenten acceder a estas páginas específicas la transmisión se bloqueará y se mandará un informe al departamento de Informática de la empresa.

Es importante recordar que el filtrado sólo protege a la empresa de un pequeño porcentaje de estas amenazas. Para una protección más completa, el dispositivo debe inspeccionar el tráfico bi-direccional en tiempo real para proteger de forma proactiva contra programas malignos de esas páginas que no hayan sido bloqueadas. Esto añade una capa de defensa para proteger la empresa de forma efectiva contra una infección accidental a través de páginas Web legítimas pirateadas, así como páginas corruptas que parezcan legítimas. La inspección del tráfico controla la información de entrada y de salida cada vez que un empleado visita una URL. Si un empleado llega a una página infectada el tráfico entrante despierta el dispositivo bloqueando inmediatamente la transmisión de la red.

Conclusión

Cualquier empresa conectada a Internet tiene que hacer frente a amenazas de seguridad basadas en Web como algo normal en sus actividades diarias. Si una empresa carece de un Gateway de Seguridad completo el riesgo es mucho mayor. Establecer y respetar una política de uso de Internet aceptable y unirlo a un control de tráfico bi-direccional en tiempo real de forma proactiva puede ayudar a reducir este riesgo.

Solución de Gestión ProSecure™ STM contra Amenazas Web y E-mail de NETGEAR®

El dispositivo ProSecure STM utiliza una tecnología única que detecta y bloquea las intrusiones basadas en un comportamiento de distribución rápido y a gran escala. De este modo se puede detectar intrusiones de spam y programas malignos tan pronto como se produzcan y bloquear todos los mensajes asociados en tiempo real.

El dispositivo ProSecure STM con tecnología Stream Scanning, está diseñado para escanear flujos de información a medida que van entrando en la red. NETGEAR STM con la tecnología Stream Scanning es capaz de procesar grandes volúmenes de información en tiempo real, utilizando un simple escáner para identificar spam, programas malignos, brechas de seguridad o aplicaciones innecesarias. Así se asegura que los usuarios de la red reciban su e-mail y los contenidos Web limpios y sin retrasos.

El dispositivo ProSecure STM utiliza un sistema de comportamiento de defensa proactivo que soluciona las vulnerabilidades. La solución NETGEAR utiliza un análisis forense para identificar características sospechosas tanto en el tráfico de entrada como de salida de la red y neutralizarlas hasta que puedan ser examinadas más detenidamente.