

Un sistema de capas de defensa ofrece seguridad completa frente a las amenazas de Internet

Introducción

Los portaaviones utilizan una completa estrategia de defensa de capas, comenzando con una detección proactiva. El radar se utiliza como la primera línea de defensa para detectar la aproximación de cualquier enemigo. Cuando se descubre una amenaza, el portaaviones emplea un mecanismo apropiado de defensa, como pueden ser misiles tierra-aire. Así mismo, el radar hace de guía a las ametralladoras para proteger la embarcación de los ataques. Cada una de estas defensas juega su propio papel, trabajando en grupo y asegurando que si alguna de ellas falla no suponga la pérdida de la embarcación.

De igual manera, los responsables de informática deben emplear una completa estrategia de capas. En vez de pistolas, misiles y otras armas de fuego tradicionales, las amenazas basadas en Internet emplean aplicaciones de software maliciosas, conocidas como programas malignos. Los programas malignos incluyen amenazas como virus, software espía, gusanos, troyanos, puertas traseras y *keyloggers* que se propagan a través de e-mail y la Web. Durante los últimos años las amenazas combinadas con dos más tipos de programas malignos, se han hecho más populares.

Los responsables de informática han utilizado durante mucho tiempo, antivirus, anti-software espía, y otros productos de seguridad a nivel de puesto informático como ayuda para protegerse contra las amenazas basadas en Internet. Aunque en su día esta protección era la adecuada, en los últimos años el mundo de las amenazas ha experimentado un gran crecimiento. Los expertos en seguridad recibían aproximadamente unos 500.000 ejemplos de programas malignos en el año 2000, pero para finales del 2008 se estima que habrán recibido unos 15 millones. Continuamente están saliendo nuevos tipos de amenazas y de formas de atacar. Como resultado los responsables de informática deben desarrollar unas medidas de seguridad que consideren esta amplia gama de amenazas. Como el portaaviones, que para prevenir de forma efectiva los ataques necesita una estrategia de capas.

El Mundo de las Amenazas

Tal y como saben los profesionales informáticos de seguridad, el mundo de las amenazas está evolucionando continuamente. Los programas malignos son más variados y complejos. Antes las amenazas sólo atacaban los puestos informáticos y tenían un ámbito y capacidades limitados, mientras que hoy en día emplean multitud de técnicas y formas de ataque a varios niveles, vía e-mail y Web a los puestos informáticos y servidores de la empresa

Los antiguos programas malignos tenían limitaciones en cuanto a lo que se podía distribuir vía floppy disks y otras formas rudimentarias, siendo los propios usuarios quienes lo distribuían de un sistema individual a otro. Hoy en día las amenazas emplean variadas técnicas de propagación, sacando provecho de la conectividad que ofrece Internet. De acuerdo a un reciente estudio Gartner, el número de amenazas Web se ha incrementado en un 800 por cien en el año 2007¹. Mientras que el e-mail se usa como forma habitual de dirigir el ataque a los usuarios. Las vulnerabilidades en el software, sistemas operativos y plug-ins de navegación ofrecen a los atacantes una forma rápida y eficaz de propagación. La conexión a Internet también permite a los atacantes exportar información sensible de los sistemas infectados de forma silenciosa.

Otra significativa evolución en el mundo de las amenazas es la intención detrás de la amenaza. Mientras que en el pasado las amenazas las desarrollaban programadores buscando impresionar a sus amigos y demás compañeros informáticos, hoy en día las amenazas las propagan criminales a cambio de dinero. Estos criminales forman parte de un creciente mercado de amenazas informáticas de 100.000 millones de dólares. Estos criminales pueden ser autores de programas malignos altamente cualificados que se alquilan para escribir el código que se necesita para el ataque, grupos criminales organizados, individuos que intentan robar información personal sensible, y dueños de listas de e-mail y otros métodos de propagación.

Esta continua proliferación del mercado criminal hace que los negocios sin protección estén en el mayor punto riesgo de los últimos años, debido a que ahora se cobra por lanzar ataques que amenazan la información sensible de la empresa y sus clientes.

La Carencia de una Seguridad Completa

En un estudio realizado en Junio del 2008, el 81 por ciento de los ordenadores de las empresas carecían de al menos uno de los componentes esenciales de seguridad, dejando el sistema vulnerable a los ataques. El estudio calculaba los niveles de seguridad de 580 sistemas buscando niveles de parches, niveles de firewalls de sistema y software de seguridad en cliente. El 63 por ciento de los sistemas no tenían instalado al menos uno de los parches críticos de seguridad de Microsoft; el 51 por ciento tenían firewalls desactivados; y el 15 por ciento tenían el software de seguridad desactivado o no estaban correctamente actualizados.

El problema no es exclusivamente de los usuarios. Otros estudios encontraron resultados similares en la parte administrativa, con niveles de protección por debajo del estándar en servidores de e-mail, servidores Web y servidores de aplicaciones. El problema es particularmente más visible en pequeñas empresas sin un departamento informático dedicado a la seguridad a tiempo completo. Ya que muchos de estos negocios no tienen experiencia en la diversidad de amenazas existentes y en las capas de seguridad que se necesitan para combatir las de forma efectiva, por ello la empresa se queda expuesta a ellas sin darse cuenta.

Delicado Equilibrio

Las seguridad y usabilidad nunca han ido de la mano. Una seguridad a prueba de tontos sería cortar toda comunicación con el mundo exterior. A pesar de que sería lo más seguro no es una solución práctica. Del mismo modo que no tener ningún control en el tráfico entrante y saliente daría a los empleados la libertad deseada, pero dejaría a la empresa a merced de los ataques. Por ello debe haber un equilibrio entre seguridad y usabilidad.

1 Estudio Gartner documento número 158459, "Por qué el filtrado de programas malignos es necesario en el Gateway Web", 26 de Agosto del 2008.

Más allá del puesto informático

Para asegurar que la empresa esté a salvo de las amenazas basadas en Internet mientras se mantiene el nivel de comunicación requerido por los empleados, se necesita una detallada descripción del problema. Con un modelo de seguridad por capas, los empleados del departamento informático evalúan los puntos de entrada potenciales e implementan una solución de seguridad específica para ese punto.

Los softwares de seguridad para el usuario final es un primer paso importante pero no es suficiente para mantener la red de la empresa segura por dos principales razones:

1. Los sistemas de usuario final no pueden controlarse de forma adecuada. Como se menciona en el estudio, los usuarios a menudo desactivan su software de seguridad o no lo actualizan de forma regular. Aunque el departamento de informática pueda realizar las actualizaciones manualmente, la tendencia creciente a tener empleados fuera de la empresa hace que esta medida no sea una solución eficiente ya que las reglas de seguridad sólo se pueden gestionar en los sistemas cuando estén conectados a la red. Si un portátil se infecta mientras está desconectado de la red de la empresa, la infección puede extenderse a través de toda la organización en cuanto se vuelva a conectar, sin que el departamento informático pueda realizar ninguna actualización.

2. El Gateway de Internet es el punto principal de entrada. Cuando el usuario se conecta a la red de la empresa, las amenazas por e-mail y Web deben pasar primero a través del Gateway de Internet de la empresa, antes de llegar al sistema del usuario. Bloquear estas amenazas en el Gateway de Internet es la manera de trabajar más proactiva y eficiente. Y también ofrece al departamento informático un mayor grado de control ya que estos recursos los manejan ellos mismos en vez de tener que depender de los usuarios.

Teniendo en cuenta estos puntos es imprescindible que las empresas aseguren sus Gateways de Internet para ofrecer una protección adecuada contra las amenazas basadas en Internet.

Control del e-mail

El e-mail sigue siendo la forma más popular de propagar gran variedad de amenazas. El spam, ataques de phishing y adjuntos maliciosos son los métodos empleados más comunes para introducir una amenaza en el entorno de la empresa. Además los sistemas infectados de los usuarios pueden utilizarse para enviar enormes cantidades de spam sin que el usuario lo detecte. Así que es importante inspeccionar y filtrar el tráfico del e-mail en el Gateway tanto de entrada como de salida.

El control del e-mail entrante puede ayudar a la empresa a impedir un gran número de amenazas vía e-mail, incluido el spam, virus, software espía, ataques de phishing y demás contenido inapropiado. Esto es importante ya que ofrece una línea de defensa vital para asegurar que las amenazas nunca lleguen al usuario.

El control del e-mail de salida, que a menudo se pasa por alto en las empresas, es otro de los puntos esenciales en una estrategia de seguridad por capas ya que es la única manera de saber si hay alguna infección dentro de la organización.

Protección Web

La utilización de la navegación Web se ha convertido en una parte esencial del día a día y existen muchas empresas legítimas que usan la Web para sus negocios. Sin embargo las páginas Web también son un vehículo de propagación de programas malignos y otros ataques basados en Web. El 79 por ciento de las amenazas basadas en Web se han encontrado en páginas legítimas que han sido pirateadas e infectadas con aplicaciones malignas. Además, las páginas inapropiadas a menudo contienen software espía y páginas maliciosas que pueden aparentar ser legítimas consiguen un importante número de visitantes a través de búsquedas online, ataques de phishing u otros métodos.

Para poder ofrecer un uso legítimo de Internet a la vez que se mantiene una seguridad apropiada en la empresa, se necesita un alto grado de escaneado de virus y otros programas malignos, así como el filtrado de URLs. Como ocurre con el e-mail se necesita escanear tanto el tráfico Web de entrada como el de salida. Escanear el tráfico de entrada determina si el tráfico Web intenta distribuir un programa maligno, si un programa maligno está intentando descargarse o si un usuario se está descargando un programa maligno por error. Escanear el tráfico de salida añade otra capa de defensa detectando si un programa espía intenta "llamar a casa", enviando a su autor información sensible recopilada del sistema del usuario.

Conclusión

Las amenazas basadas en Internet son un componente prominente y en crecimiento del mundo de las amenazas. Estas amenazas pueden tomar formas diversas y utilizar cualquier forma de propagación, por ello confiar solamente en una seguridad basada en puesto informático es un mecanismo de defensa inadecuado. En vez de ello, los responsables de informática deben desarrollar una política de seguridad completa para protegerse contra estas amenazas. Los responsables de informática pueden proteger la empresa de forma efectiva contra ataques vía Internet utilizando una defensa por capas y añadiendo a la seguridad por puesto informático la inspección del tráfico entrante y saliente que se realice tanto vía Web como por e-mail.

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.