

La Integración de Sistemas de seguridad



Velando por tu seguridad

La integración de sistemas de seguridad

De vez en cuando, es útil refrescar la memoria, sobre todo cuando se trata de temas de seguridad. Dicen que hay que conocer la historia para no repetir los errores pasados, y en febrero de 2006 se va a cumplir una década de un ataque con nombre curioso: "Smurfing". Supongo que muchos de los que estén leyendo esto conocerán a los Smurfs, las criaturitas azules creadas por Peyo, dibujante belga.

El ataque llamado smurfing consiste mandar una gran cantidad de "pings" a la dirección IP de broadcast de la red, todas con una dirección IP falsificada: la de una víctima. Si el router lo permite, todos los sistemas de la red responderán al ping, multiplicando el tráfico y produciendo una saturación tal en el equipo víctima del ataque que podría llegar a dejar de responder.

Evidentemente, hoy en día este ataque podría considerarse prácticamente extinto, ya que cualquier red corporativa (por pequeña que sea) dispone de un firewall en el que, seguramente, no se responde a los pings externos y no se permita así que pueda llevarse a cabo el ataque. Pero sin embargo, hay muchas otras posibilidades de lanzar un ataque sin necesidad de recurrir a los smurfs, y hay ejemplos que lo demuestran.

Uno muy claro es el llevado a cabo por el gusano SQLSlammer. Este gusano se multiplicaba a través de una instrucción dada a través del puerto 1434. Este puerto se utiliza para la comunicación entre distintos servidores SQL Server cuando deben compartir información entre ellos, por lo que en algunos casos era necesario tenerlo abierto. Pero en otros muchísimos casos (como en los que estaba instalado algún elemento de SQL Server, como ocurría con algunos clientes SQL server) ese puerto permanecía abierto sin necesidad.

Hoy en día tanto el puerto 7 como el 1434 suelen permanecer cerrados, al igual que muchísimos otros. Generalmente se dejan abiertos los puertos que son estrictamente necesarios para el funcionamiento de las empresas. Sin embargo, ¿quién nos asegura que ese puerto que necesita esa aplicación no va a dejarnos en peligro?

La solución pasa por vigilar las aplicaciones que lleven a cabo uso de los puertos abiertos en la empresa, para poder detectar un comportamiento anómalo y, si se observan problemas, cerrar la comunicación. Sin embargo, hoy en día las soluciones que pueden ofrecer la información necesaria para asegurar el sistema están dispersas en distintos dispositivos de la red.

Por un lado, los HIPS (Host-based Intrusión Prevention Systems) suelen instalarse en máquinas que no se encuentran en primera línea de la conexión. Pueden estar en un servidor interno o en una máquina cliente, en el mejor de los casos en la DMZ, pero no en la misma puerta de conexión. Para ese punto suele dejarse el firewall, que es un sistema muy estático y con una configuración preprogramada

La Integración de Sistemas de seguridad



Velando por tu seguridad

por el administrador de la red o incluso por un proveedor de seguridad externo, pero es independiente de otros sistemas de protección.

La seguridad que exigen los administradores de red en estos momentos necesita una velocidad de reacción que el modelo actual no ofrece. El tiempo que puede pasar entre que un sistema detecte una intrusión y el administrador decida cerrar el puerto correspondiente en el firewall puede ser excesivo y con consecuencias desastrosas. No estamos hablando de unas horas, sino un tiempo inferior al que puede tardar un administrador en teclear su contraseña y entrar en la consola de administración del sistema de seguridad: simplemente, segundos.

La solución pasa por llevar a cabo una integración de dispositivos que aúne todas las tecnologías en un solo sistema. Un firewall es muy útil, pero necesita una actualización de reglas continua, un HIPS no protege contra amenazas desconocidas. Sin embargo, las dos soluciones integradas pueden ser la solución a la situación de las amenazas en este momento. Y no sólo el HIPS y el firewall, sino que la integración de aplicaciones de seguridad debe incluir también una solución antivirus clásica, con capacidad de detección de otro tipo de amenazas, como spyware, spam, phishing...

En estos momentos, la situación de la seguridad informática requiere una nueva orientación en los sistemas de seguridad. Los creadores de malware han dado un salto importante en sus objetivos y ya no solo está en juego nuestra información, sino directamente nuestro dinero. El acceso a los sistemas informáticos por parte de hackers ya no busca el afán destructivo por que sí, sino que hay una clara razón para intentar introducirse en un servidor empresarial: el dinero.

Y más aún, podemos encontrarnos con un ataque dirigido expresamente a un sistema en particular, por lo que hay que contar con todas las herramientas de seguridad juntas en un solo punto de la red: precisamente la entrada de Internet. Si la protección está más atrás o está repartida por distintos sitios, nos podremos encontrar que no va a respondernos con la eficacia que necesitamos.

La unificación de protecciones en un punto tan crítico como la entrada de Internet abre el camino a un concepto de prevención contra todo tipo de ataques e intrusiones a nivel de la red global que se pretende proteger. Este concepto es denominado NIPS (Network Intrusion Prevention System o Sistema de Prevención de Intrusiones a nivel de Red) y es hoy por hoy la garantía de implementar una protección eficiente para cualquier red empresarial.