



Sistemas IPS: nuevas soluciones para amenazas recientes

La industria del cibercrimen es cada vez más compleja y no cesa en la búsqueda de nuevas formas de infectar sistemas y asaltar redes corporativas. Los ataques modernos llegan de forma combinada y desde diversos frentes, valiéndose de tácticas internas y externas. Ante este contexto, los sistemas de prevención de intrusiones (IPS) se sitúan en la primera línea de batalla y dotan de escalabilidad a nuestra defensa.

Con ellos, es posible proteger las redes y los servidores de forma proactiva, gracias a la monitorización y a la gestión central. Al vigilar el tráfico de red y monitorizar cuanto sucede en su interior, es posible detectar un ata-

sólo cubren los niveles 3 y 4 y no son capaces de detectar ataques a raíz de la carga que contengan los paquetes de datos.

Un IPS detiene única y exclusivamente el tráfico malicioso nada más detectarlo, sin perjudicar al resto de tráfico legítimo y, por ende, permitiendo que la red siga funcionando sin problemas. Así, se asegura la operatividad en caso de que se produzca un fallo y se dota al negocio de la tan necesaria continuidad que demanda el mercado hoy en día.

La seguridad interna, al nivel de la perimetral
Frente al valor que siempre se le ha otorgado a la seguridad perimetral, encargada de velar por



que en cuanto comienza a producirse e, incluso, ser capaces de anticiparse a él. Examinando las conexiones tanto desde el punto de vista del cliente como desde el punto de vista del servidor, se pueden detectar anomalías al instante y tomar decisiones en consecuencia, sin que ello afecte a las conexiones normales, que nunca, bajo ningún concepto

un adecuado control de accesos y de la erradicación de las intrusiones, la seguridad interna cobra ahora la importancia que se merece ante la difuminación que el propio perímetro ha experimentado en los últimos años. Con la llegada de las redes inalámbricas, los dispositivos móviles y demás elementos ajenos en principio al propio perímetro, las empresas son ya conscientes de la necesidad de protegerse desde dentro de igual forma que venían haciendo hacia el exterior.

Sin ir más lejos, un ordenador infectado fuera de nuestra red y posteriormente conectado a ella habría burlado al firewall más exigente. Para evitar que el código malicioso se difunda entre el resto de los equipos conectados a la red, es imprescindible contar con sistemas que inspeccionen tanto el tráfico externo como el interno. Ambos son igual de importantes, en la medida en que los dos son capaces de constituir una amenaza.

Por ello, los gestores inteligentes y los departamentos TI más avanzados recurren desde hace tiempo a los IPS. Su capacidad, efectividad y nivel de protección están fuera de toda duda, habiéndose convertido por derecho propio en uno de los aliados más potentes en cuanto a seguridad corporativa se refiere.

“Los sistemas de prevención de intrusiones dotan de escalabilidad a la defensa”

deberían ser cortadas por ningún dispositivo, ya que sería lo mismo que hacernos una denegación de servicio a nosotros mismos.

Esto resulta particularmente útil en el caso de estar expuesto a alguna vulnerabilidad todavía no parcheada, pues el IPS reacciona creando una nueva política de seguridad, que aplicará de forma automática en el caso de repetirse un ataque similar en el futuro.

Su protección abarca desde el nivel 2 (control de acceso al medio) hasta el nivel 7 (aplicación), con lo que ofrecen una protección superior a la de los simples cortafuegos, que