La (otra) realidad de los Sistemas de Detección de Intrusiones

Autor: Sebastián García – CYBSEC S.A. (*)

Un Sistema de Detección de Intrusiones (IDS) básicamente es un programa que intenta detectar comportamientos anómalos en nuestra red, que podría significar que un intruso esté actuando sobre la misma. Decimos **intenta** porque ningún programa es perfecto y en realidad no sabemos cuantas veces falla; **comportamientos anómalos** se refiere a que algunas computadoras o usuarios tengan un comportamiento anormal, indeseado o en contra de los intereses de la empresa; **intruso** es alguien que lleva adelante el ataque, independientemente si se encuentra vinculado o no a la Empresa.

En esta definición básica ya se perciben algunas dificultades, la más importante es definir qué es algo indeseado o en contra de los intereses de la empresa, los IDS no lo saben y esperan que nosotros se lo digamos a través de configuraciones y ajustes. Cuando se trabaja con IDS debemos tener conocimientos de su operación y configuración, del tráfico de red normal existente, de que acciones se deben vigilar y cuales no. El objetivo es volcar en la práctica las políticas de detección de intrusiones.
Un IDS mal configurado no nos beneficiará mucho, será una molestia o en el peor de los casos, tendremos que desactivarlo por la cantidad de información inmanejable que nos brindará.

La instalación, configuración y ajuste de un sistema IDS requiere tiempo y dedicación. Es una tecnología nueva y en crecimiento, todavía veremos muchos avances en los próximos años. Lo más importante es que no hay que pensar que los problemas de detección de intrusiones están resueltos por instalar un sistema de IDS.

Los principales problemas en una organización cuando se instala un IDS son:

1. No se conoce como trabaja realmente el IDS.
2. No se conoce cuantas veces falla en la detección.
3. No se conoce el tráfico normal de la red a proteger.
4. Se confía en un solo producto de IDS.

5. Se instala y configura el IDS y no se lo vuelve a actualizar.

El no conocer como trabaja un IDS impide que entendamos como se debería configurar correctamente, y como se debería reconfigurar y actualizar a medida que pasa el tiempo.

Los IDS miden su eficiencia por dos valores, los falsos positivos (cuando detectan un ataque que no era tal) y los falsos negativos (cuando no detectan un ataque que era tal). Como los falsos positivos son preferibles a los falsos negativos, ya que preferimos tener información de más a no detectar un ataque real, la mayoría de los IDS tienen una alta tasa de falsos positivos en sus detecciones normales, pero lo que no se da a conocer comercialmente es que los IDS también tienen una alta tasa de falsos negativos, lo que es una potencial ventaja para el intruso.

Según las investigaciones realizadas en el CISIAR (Centro de Investigación en Seguridad Informática Argentina) casi el 50% de los ataques realizados contra el IDS Snort no fueron detectados por el mismo, teniendo en cuenta que se considera el IDS de distribución libre más actualizado y veloz del mercado.

Durante el proceso de instalación de un IDS, lo primero que hay que analizar es el tráfico de red del segmento donde colocaremos el IDS, evaluando que protocolos están pasando por la red (muchos IDS solamente analizan ataques a nivel del protocolo TCP/IP) y cual es el tipo de tráfico (un IDS no puede analizar el contenido de una sesión HTTPS o IPSEC). Con esta información se va a tener una idea más clara de lo que se desea monitorear.

Otro de los problemas en las empresas es confiar la detección de intrusiones en un IDS solamente. En el mercado existe una gran variedad de sistemas de detección de intrusiones, la gran mayoría comerciales que se autopromocionan como “la mejor solución”. Es altamente recomendable evaluar el IDS a implementar. Por ejemplo, utilizando dos IDS diferentes sobre el mismo segmento de red y al mismo tiempo, hemos detectado significativas diferencias en falsos positivos y negativos.

Un IDS instalado con su configuración por defecto es una herramienta de doble filo, ya que nos invadirá con gran cantidad de falsos positivos. En este caso debemos ser capaces de:

- Conocer que es lo que debería pasar y lo que realmente sucede en la red de mi

organización.

- Configurar y hacer el ajuste sobre el IDS para que solo detecte los probables intentos de intrusión.

Este último punto debería realizarse cada cierto período de tiempo. La seguridad informática en su conjunto es dinámica y la detección de intrusiones como una de sus áreas especializadas concentra la mayor parte de su dinamismo. Todos los programas de IDS permiten realizar una actualización de firmas de ataques, que incluyen los últimos tipos de ataques detectados.

A modo de conclusión, cabe destacar que es de vital importancia que una empresa tiene que capacitar a las personas que estarán a cargo de detectar intentos de intrusión, debe saber que IDS utilizar, como instalarlo, configurarlo y ajustarlo correctamente de acuerdo a sus requerimientos.

Siempre hay que tener en cuenta que un Sistema de Detección de Intrusiones es simplemente una herramienta que nos brinda una excepcional ayuda en la difícil tarea de mantener la seguridad de nuestros sistemas informáticos.

En la realidad, todavía no existe la solución “Plug & Play” en la tecnología IDS, el correcto resultado final solo se consigue con tiempo y dedicación. Pero al final, los resultados son gratificantes.

Sebastián García es Consultor Senior de CYBSEC Security Systems, donde se dedica a investigar e implementar sistemas de detección de intrusiones. E-mail: sgarcia@cybsec.com.