Sistemas de detección de intrusión en la red para infraestructuras críticas

Daniel Paillet, Schneider Electric, *www.schneider-electric.com.ar*

Los asaltos en contra de las redes de infraestructura crítica están creciendo en lo que a sofisticación se refiere y requieren perímetros de defensa más fuertes. Aunque los firewalls ofrecen un buen grado de seguridad en los límites por filtrar el tráfico, estos sistemas pueden pasar por alto ataques más avanzados que llegan desde dentro o fuera de la red. Los sistemas de detección de intrusión en la red (NIDS), por otra parte, proveen una capa adicional de profundidad a la estrategia de defensa. Este artículo repasa cómo los NIDS defienden en contra de los ciberataques.

Introducción

Las infraestructuras críticas (por ejemplo, redes de energía, redes de agua, sistemas SCADA de fabricación) se están convirtiendo en un objetivo privilegiado para los ciberataques generados por individuos, grupos delincuentes y estados nacionales. Estos ataques están creciendo en intensidad y sofisticación y son capaces de cambiar la configuración del sistema o destruir sistemas que son críticos para nuestra vida moderna. Los sistemas hospitalarios, energéticos o de agua son particularmente vulnerables a este tipo de ataques.

De acuerdo con Warwick Ashford de *computerweekly.com*, "Las organizaciones de infraestructura crítica son el objetivo común de ciberataques que buscan manipular equipamiento o destruir antes que robar información".

Una encuesta de la Organización de los Estados Americanos y la empresa de seguridad *Trend Micro* entre aproximadamente quinientos proveedores de infraestructura crítica reporta que el 44 por ciento ha detectado intentos de borrar archivos. Además, el sesenta por ciento de las organizaciones encuestadas dijo que ha detectado intentos de robar información y el 53 por ciento notició un incremento en los ataques a sus computadoras durante 2014. La encuesta reveló que el 76 por ciento sentía que los ataques en contra de la infraestructura eran cada vez más sofisticados.

Los sistemas que defienden en contra de tales ataques se presentan en todas las formas y tamaños. Los niveles de seguridad que se alcanzan varían enormemente dependiendo del grado de implementación. Este artículo presenta una estrategia de defensa centrada en NIDS. La figura 1 ilustra una arquitectura planificada y profunda y muestra dónde se ubica NIDS.

El rol de la detección de intrusos en la red

Muchos de los firewalls de gestión de amenaza unificada (UTM) de la próxima generación cuentan con capacidades de detección de intrusión y prevención de detección de intrusión. Estos sistemas pueden ser efectivos para proteger los límites de la red contra el tráfico malo. Sin embargo, si ocurriera un ataque dentro de una subred interna o en la red virtual de área local (VLAN) interna, el firewalll ubicado en los límites externos no podría detectarlo. Esta es la razón por la cual los NIDS son valiosos y

Daniel Paillet

Daniel Paillet es actualmente arquitecto jefe de ciberseguridad en Schneider Electric. Su trayectoria incluye haber trabajado en varios proyectos de seguridad para el Departamento de Defensa de Estados Unidos. Cuenta con quince años de experiencia en el área de seguridad de tecnología de la información y tecnología operacional. Cuenta con CISSP, CEH y otros certificaciones específicas de vendedores. Actualmente, se dedica a desarrollar y mejorar ofertas y soluciones de seguridad dentro de *Schneider Electric*.

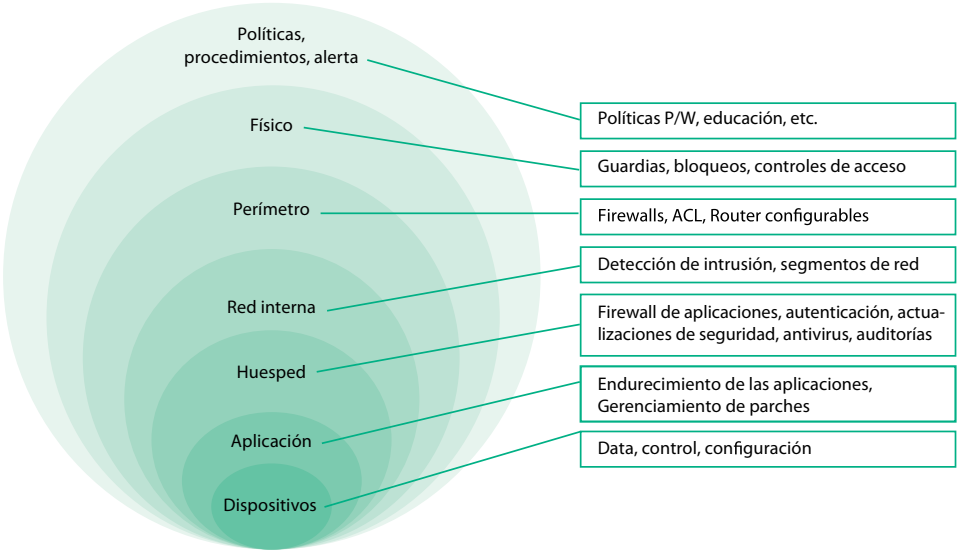

Figura 1. Arquitectura de seguridad que incorpora varios niveles

necesarios para proteger redes de infraestructura crítica. Si la próxima generación o firewalls basados en UTM perdieran un ataque proveniente del exterior, el NIDS proveería una capa adicional de defensa.

Los NIDS se desempeñan en los puntos de entrada clave en una red y reportan su información a un servidor central en donde las alertas aparecen sobre una consola. En estos servidores, en general corre una base de datos SQL en donde se almacenan las alertas y reportes. Los analistas entrenados en visualizar tales alertas estarán mirando el tráfico de la red para determinar si las alertas son ataques legítimos. En el caso de un ataque, el equipo de defensa de la red llevará a cabo la acción apropiada para resistir el ataque de acuerdo a procesos y procedimientos internos de las organizaciones.

Los sistemas de detección de intrusión utilizan tres metodologías de detección diferentes:

- Detección en base a firma: el NIDS detecta firmas que se correspondan con los patrones de amenazas conocidas. La detección basada en firmas está limitada en su efectividad en que solo es tan buena como la más reciente actualización de firmas lanzadas por el fabricante.
- Detección basada en anomalías: en la detección basada en anomalías, el NIDS compara la actividad normal con los eventos que observa e identifica como desviaciones significativas. Se generan alertas a través de métodos estadísticos que comparan la actividad del momento con la actividad previa. Esto se puede ajustar en base a investigación y observación.
- Análisis de protocolo del firewall con estado: en este método, el NIDS observa la mecánica de protocolos específicos para determinar si el tráfico se condice con los estándares de protocolo. Por ejemplo, un mensaje de "conectar" de un solo cliente repetido durante un breve lapso de tiempo podría indicar un ataque de "denegación de servicio" (DoS). Esto también puede incluir una inspección profunda de paquete (DPI) para revisar cualquier paquete malicioso en la red.

Los sistemas de detección de intrusión están diseñados para monitorear y alertar cuando detectan

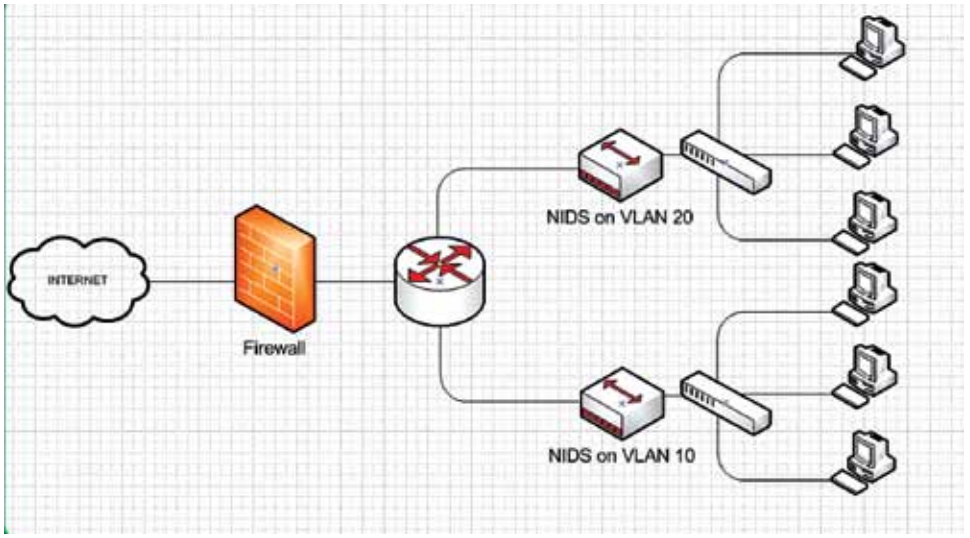

Figura 2. Típica locación de NIDS dentro de una red

un patrón o una determinada firma inusual. Un analista debe investigar y determinar si la alerta es un falso positivo o un ataque potencial contra la red. Las grandes organizaciones tienen analistas observando el tráfico desde NIDS en una base 24/7 (todo el día, a toda hora). Algunos analistas han sido entrenados y han desarrollado la técnica de escribir firmas comunes para capturar más detalles del análisis del tráfico de red, y para revelar ataques sofisticados ocultos enviados por entidades desde fuera o dentro.

Conclusión

La implementación de NIDS dentro de las redes varía según la organización y el sitio. El presupuesto es una cuestión considerable en y está ganando el soporte de la dirección para su desarrollo. Otras consideraciones incluyen:

- Identificación de los vendedores apropiados con experiencia en el área de infraestructura física de ciberseguridad
- Locación de los sensores NIDS
- Determinación sobre qué normas de seguridad existen para atender incidentes
- Entendimiento de la red: detección de tráfico y mecanismos de respuesta activos
- Administración de NIDS: instalación de gestión y mantenimiento
- Reclutamiento y entrenamiento de analistas para monitorear el tráfico
- Monitoreo de operaciones cuando se requiere 365/24/7
- Establecimiento de un proceso de respuesta ante incidentes cuando se descubre uno
- Determinación acerca de si la contratación de una administración y análisis de NIDS tiene sentido, y si la respuesta es positiva, cómo negociar el acuerdo de nivel de servicio (SLA).

La puesta a punto también jugará un rol relevante en las etapas más tempranas de implementación de un NIDS. El rol del analista es importante para determinar qué alertas son falsos positivos y cuáles son ataques legítimos. Esta parte de la implementación puede ser muy extensa e intensa. Una vez que el NIDS se pone a punto (y a veces la puesta a punto es un proceso permanente, dependiendo de la red), se creará una capa extra de defensa como parte de la arquitectura de la red. ❖