Integración de herramientas de gestión de red y de seguridad

En este artículo se comentan algunas posibilidades de integración entre las herramientas de gestión de red y sistemas o agentes específicos de seguridad. Aunque parte de esta integración, especialmente la referida a la recolección de alertas de forma centralizada, no es un asunto nuevo, sí es cierto que en la gran mayoría de los casos el aprovechamiento de las plataformas de gestión se limita a tal centralización de alarmas, cuando potencialmente sus posibilidades son mucho mayores. En Germinus Solutions, la estrecha colaboración entre las Divisiones de Infraestructura de Red y Seguridad ha hecho posible el diseño e implantación de soluciones con un valor añadido muy superior, y que por tanto ofrecen un mejor aprovechamiento de la inversión realizada.

Javier Fernández-Sanguino / Antonio Requejo

Las herramientas de gestión, no sólo de equipamiento de red sino también de sistemas finales, son una solución a las necesidades de operación y mantenimiento de la gran mayoría de las empresas. Independientemente del producto utilizado por la organización éstos van a poder realizar, entre otras tareas:

– monitorización activa de sistemas y de su disponibilidad.

– recepción de eventos y ficheros de registro (*logs*) generados por los sistemas.

– sistemas expertos para determinación de fallos (generalmente a través de correlación de eventos)

– gestión remota de sistemas a través de agentes.

Habitualmente, cuando se habla de gestión de red se hace fundamentalmente de arquitecturas basadas en SNMP; sin embargo, al hablar de gestión de sistemas se introduce, en la gran mayoría de los fabricantes, desarrollos de agentes específicos para las plataformas a monitorizar.

Las herramientas de gestión de seguridad realizan las mismas tareas pero únicamente desde el punto de vista de la seguridad. Es decir, reciben eventos de seguridad, los agregan y correlacionan, gestionan las políticas de seguridad de forma remota, y pueden gestionar también la autenticación de usuarios (proporcionando servicios de *single-sign-on*). En general, un sistema de gestión de seguridad deberá ayudar a la implementación del ciclo de 'prevención', 'detección' y 'respuesta' que defina la política de seguridad corporativa.

¿POR QUÉ INTEGRAR?

La respuesta no es nada original. El objeto de la integración es la obtención de un sistema final integrado mejor que la suma de los sistemas separados. Se busca, pues, sinergia. La "mejoría" conseguida puede ser percibida en diferentes aspectos. En este caso, el ahorro de costes y la eficiencia son los principales beneficios percibidos.

Se ahorran costes, porque se elimina la necesidad de nuevos productos (y de sus plataformas correspondientes) y de nueva formación para administradores y personal de soporte. Se aprovecha mejor lo que ya tenemos, o en otros casos, se justifica más la inversión.

Se mejora en la eficiencia pues la información de seguridad se incorpora al flujo de información general sobre la infraestructura que ofrece la plataforma de gestión de red, completándola y ofreciendo posibilidades de correlación que enriquecen el resultado y la visión que se tiene en cada momento sobre nuestra red.

¿POR QUÉ INTEGRAR CON GESTIÓN DE RED Y SISTEMAS...?

... frente a montar un sistema aislado de gestión de seguridad? Existen en el mercado plataformas de gestión centralizada de información de seguridad (consúltense las referencias para más información), que ofrecen, quizá de forma más directa, parte de lo que aquí se comentará. Evidentemente, estos productos han sido diseñados para realizar gestión específica de seguridad pero su introducción dentro del entorno de operación de una empresa puede ser traumática por la necesidad de reconfigurar dispositivos para incluirlos dentro de esta gestión y por la de formar a personal para el manejo de una nueva herramienta.

Figura 1: Gestión de seguridad dentro de la gestión de red

La respuesta a la pregunta, sin embargo, puede ser tan sencilla como que la empresa ya dispone de una plataforma de gestión de red y sistemas implantada que funciona adecuadamente. En este caso puede que ésta quiera funcionalidades que no le ofrece un producto específico de gestión de seguridad, o puede que quiera justificar la inversión (económica y en formación del personal). Es más, la gestión de seguridad desde una herramienta general es, en algunos casos, el primer paso para la utilización posterior de un producto específico de gestión de seguridad con un cierto grado de acoplamiento.

EVOLUCIÓN DE FABRICANTES DE SISTEMAS DE GESTIÓN TRADICIONALES

Sin embargo ésta respuesta no es la única que puede darse. Las herramientas de gestión (consúltense las referencias para más información) vienen ofreciendo la capacidad de gestionar aplicaciones, comunicaciones, dispositivos de almacenamiento y sistemas operativos con la intención de proporcionar información de operaciones, disponibilidad o rendimiento. Añadir "seguridad" a este portafolio es una evolución natural.

Así, los fabricantes de productos de gestión tradicionales están avanzando en la integración o implementación de productos de apoyo a la gestión de seguridad. Algunos fabricantes, como por ejemplo HP con su plataforma de gestión Openview, está intentando lograr esto a través de alianzas e intercambios tecnológicos con compañías especializadas en productos de seguridad. Por ejemplo, HP Openview firmó recientemente una alianza con Internet Security Systems para integrar el correlador de eventos de seguridad dentro de la plataforma de gestión HP Openview Operations. Otros fabricantes están implementando sistemas de gestión de seguridad basados en (e integrados con) los sistemas de gestión propia de los fabricantes. Por poner algunos otros ejemplos, éste es el caso de Aprisma con su producto Spectrum Security Manager o de Tivoli con Risk Manager e Intrusion Manager.

En cualquier caso, la flexibilidad dada en estos sistemas de gestión es, por regla general, superior a la ofrecida por las herramientas de gestión de seguridad. Esta misma flexibilidad puede ser una razón por sí sola para realizar la gestión de seguridad (total o parcialmente) en base a estas herramientas. En función de las necesidades de la organización, una solución cerrada (o limitada) puede no ser suficiente para llegar a implementar, por ejemplo, los métodos de tratamiento ante incidentes definidos por la política de seguridad o cualquier otro procedimiento. Es difícil que una herramienta de seguridad genérica pueda adaptarse "de serie" a cualquier política de seguridad. Como reza el dicho: "en la variedad está el gusto", sin embargo, esta misma variabilidad es la que hace necesario la realización de desarrollos (y adaptaciones) adicionales a cualquier plataforma de gestión.

Esta misma flexibilidad da lugar a la oportunidad de ofrecer nuevas e interesantes propuestas de funcionalidades desarrolladas sobre las plataformas de gestión integrando distintos elementos que pudieran coexistir en la infraestructura de la organización. Se pueden implementar distintos modelos de integración como algunos de los que se describirá a continuación.

INTEGRACIÓN CON ANÁLISIS DE VULNERABILIDADES

La integración de los eventos de seguridad y los sistemas de análisis automático de vulnerabilidades es una interesante e imaginativa posibilidad a incorporar en la plataforma de gestión de red. De hacerla

sería posible, por ejemplo, que al recibir un evento de seguridad (un ataque) dirigido contra un equipo podría incrementarse (o reducirse) la prioridad de dicha alarma porque se conoce que el dispositivo es (o no es) vulnerable a este ataque específico.

Ésta es una funcionalidad que ya ofrecen, de hecho, algunos sistemas de detección de intrusos. Así, Dragon (Enterasys Networks) puede correlar las alarmas con Nessus y RealSecure (Internet Security Systems) puede correlar las alarmas con Internet Scanner. Los sistemas de gestión son mucho más flexibles, permitiendo la integración de herramientas de análisis de vulnerabilidades con sistemas de detección de intrusos, con independencia de los fabricantes. En el caso de que, además, se utilice una herramienta de detección de vulnerabilidades y de detección de intrusos *open source*, como Nessus y Snort, es posible lograr resultados más adaptables a las necesidades existentes.

INTEGRACIÓN CON INVENTARIOS DE SISTEMAS

Es de destacar que los sistemas de gestión de red y sistemas tienen la capacidad de generar un sistema de inventario gracias a sus funciones de auto-descubrimiento de los equipos presentes en la red. Este inventario de sistemas, habitualmente desaprovechado, tiene una gran utilidad como información adicional que puede ser correlada con la información de seguridad recibida.

Así, otra posibilidad de gran interés es la integración de los eventos de seguridad con estos mismos inventarios de sistemas. En este caso se puede utilizar la información de estos repositorios cuando, por ejemplo, se recibe una alerta de un sensor IDS de red de un ataque a un servidor de DNS relacionada con el sistema de correo interno (cuyo inventario no incluye la existencia de este tipo de servidor). Este análisis automático permite descartar la alarma (o reducir su prioridad) por considerarla un falso positivo, permitiendo hacer frente a los problemas de generación de falsos positivos de este tipo de sensores. De esta forma se reduce la sobrecarga de información a la que pueda estar sometido un operador de seguridad por parte de los sistemas de detección de intrusos.

CORRELACIÓN ENTRE EVENTOS DE DISTINTA NATURALEZA

Esta integración (en la forma de correlación) entre eventos no específicos de seguridad y eventos de seguridad puede llegar a ser una de las más complejas pero que más aporte a la calidad de la información proporcionada sobre la evolución de un ataque. Sólo es posible, sin embargo, si está claramente definida y se dispone de suficiente información de la infraestuctura como para diseñarla.

Habitualmente un problema de seguridad que no ha sido detectado puede trasladarse al resto de la infraestructura y, por tanto, puede darse el caso de que se generen eventos que no son de seguridad pero que tienen su raíz en un problema de seguridad. Si se realiza una correlación de estos eventos, se puede "detectar" el problema y dar la oportunidad de tratarlo eficazmente. Se pueden evitar las consecuencias de la aparición de "falsos negativos" en los detectores de intrusos, ya que estos eventos se detectarán por su impacto en los sistemas.

También es posible correlacionar información de eventos de seguridad (un ataque sobrecarga de 'búfer') con un evento que no es de seguridad (aumento de la carga de proceso de un equipo) para determinar una situación más compleja (un intruso que está ejecutando tareas en un sistema gracias a un ataque).

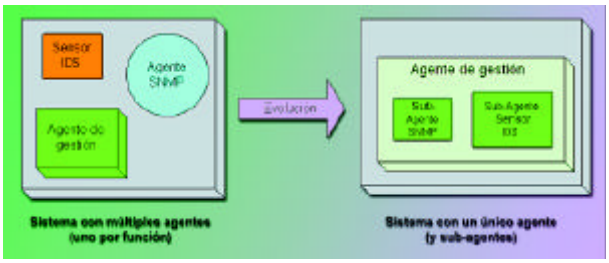

Figura 2: Posible evolución de las arquitecturas de agentes

Hay que destacar que esta funcionalidad de correlación la realizan los sistemas de gestión de seguridad y que, por tanto, la profundidad de correlación dependerá de sus capacidades. Podrán hacerla en eventos de seguridad enviados por distintos dispositivos pero no necesariamente con eventos que no son de seguridad. Puede que no reciban estos eventos y que, aunque los reciban, no soporten los dispositivos que los generan (no saben interpretarlos). Nuestra experiencia en este caso muestra que se es muy dependiente de la flexibilidad del producto en sí a la hora de poder implementar esta integración.

INTEGRACIÓN CON SISTEMA DE CONTROL DE ACCESO FÍSICO

En el caso de disponer de un sistema de control de acceso a salas mediante dispositivos electrónicos, es posible correlar la información enviada por estos dispositivos cuando accede un usuario con la misma información de acceso proporcionada por los sistemas de información. De esta forma sería posible determinar que es un acceso inválido el acceso a un sistema de información por el usuario X cuando el que ha accedido a la sala es el usuario Y. Lo que algunas veces se observa en películas de Hollywood, en la que desde una consola gráfica se pueden seguir los pasos de un usuario por el edificio, no es ni mucho menos descabellado. Por supuesto, como en todos los casos que estamos comentando, hay que disponer de los dispositivos adecuados y del *know-how* para realizar dicha integración. Aunque esta posibilidad ha sorprendido en más de una ocasión que se ha propuesto, examinada de forma aséptica no es más que una correlación de información entre el mundo "lógico" y el "físico", que incluso a veces se realiza manualmente.

INTEGRACIÓN CON OTRAS FUENTES DE INFORMACIÓN

Se puede utilizar, incluso, otras fuentes de información de seguridad externas a la organización con el sistema de gestión. Estas fuentes de información podrían ser listas de correo-e (como las de los fabricantes en cuanto a alertas sobre sus productos), bases de datos de vulnerabilidades (como las de CVE, CERT, ISCAT, Bugtraq, Alerta-antivirus.es), etc.

En este caso, se puede definir un sistema de recuperación y normalización de esta información, bien a través de filtros de correo que traten los recibidos de servicios de alertas, bien a través de herramientas que descarguen las últimas vulnerabilidades encontradas en bases de datos. Una vez normalizada la información, puede ser correlada con el inventario existente en el servidor de gestión. Así, por ejemplo, al recibir un correo de un fabricante avisando de un problema de seguridad en una versión determinada de sus *routers* se puede generar una alerta asociada a aquellos equipos en la organización que coinciden con ese mismo modelo y versión de sistema operativo. De esta forma frente a un solo evento, como es una alerta de seguridad de un fabricante, se pueden generar tantas alertas como sistemas existan que coincidan con la descripción dada por el fabricante, eventos que deben ser tratados por el operador de seguridad asignado. (ver **Tabla 1**)

IMPLEMENTACIÓN DE GESTIÓN DE SEGURIDAD EN UNA HERRAMIENTA DE GESTIÓN GLOBAL

Vistas las posibilidades, ¿cómo implementar gestión de seguridad?

Una implementación posible, para aquellas organizaciones que deseen "exprimir" al máximo (y rentabilizar) su sistema de gestión de red y sistemas es convertir éste en un sistema de gestión de seguridad. Para esto es necesario revisar, inicialmente, si el sistema de gestión está ya recibiendo o no alarmas de seguridad de dispositivos heterogéneos, qué alarmas que está recibiendo (y que no son de seguridad) son aplicables a dicha gestión y qué dispositivos de seguridad pueden hacerse interoperar con el sistema de gestión. En este caso, en última instancia seguramente todos sean integrables, debido al despliegue de agentes de SNMP y envío de *traps* de SNMP por parte de estos sistemas de seguridad; sin embargo, la integración mediante agentes SNMP puede no ser la más recomendable (por las deficiencias de seguridad conocidas en este protocolo). Una vez se definan qué eventos se reciben (o pueden recibirse) es necesario determinar si éstos pueden tener relación entre sí, y, caso de tenerla, definir las correlaciones necesarias para sacar un aprovechamiento máximo de esta información.

Una vez se tiene el sistema de gestión y los sistemas gestionados configurados para poder empezar a utilizarlo como sistema de gestión de seguridad llega la gran pregunta: "¿quién se hace cargo de los eventos de seguridad?". Claramente, la función de operación de seguridad es una labor separada (aunque relacionada) con la operación y mantenimiento de los sistemas en sí. Esta última tarea será realizada por un personal pero no necesariamente por el mismo que vaya a realizar la gestión de seguridad, personal que habitualmente contará con un perfil muy específico o, incluso, personal que no formará parte de la organización por ser un servicio ofrecido por una empresa de seguridad gestionada.

Integrado con...	Complejidad	Aportación
Análisis de vulnerabilidades	Media	Reducción de falsos positivos en alertas.
Sistema de inventario	Baja	Reducción de falsos positivos en alertas.
Contro de acceso físico	Media/Alta	Mayor granularidad en el control de acceso
Fuentes distintas de eventos	Alta	Detección de falsos negativos.
Fuentes de información externas	Media/Alta	Gestión proactiva de la seguridad

Tabla 1 Nuevas posibilidades de integración y su aportación a la seguridad

Así pues, se deberá configurar el sistema de gestión con los perfiles de operadores que vayan a recibir alarmas de seguridad, de forma que atiendan específicamente a estas alarmas (y no necesariamente otras). Estos operadores podrán, o no, tener acceso al resto de la información residente en el sistema de gestión. Todo esto puede suponer un trabajo arduo de definir qué procedimientos de operación se van a implantar para dichos operadores, procedimientos que deberán estar soportados en la política de tratamiento de incidentes dentro de la política de seguridad corporativa. (ver **Figura 1**)

DESPLIEGUE DE AGENTES DE SISTEMAS

Los agentes propietarios ofrecidos por las herramientas de gestión de sistemas son, por regla habitual, extremadamente versátiles y extensibles. Esto es así porque dichos agentes deben ser parametrizados para cubrir las necesidades de monitorización que los usuarios de dichas herramientas demanden. Por otro lado distintos elementos de seguridad, como puedan ser los detectores de intrusos de *host*, se basan también en agentes en las plataformas.

Sin embargo, la utilización del propio agente de gestión como agente de detección de intrusos (extendiendo las capacidades de éste) ahorra la instalación de un nuevo agente en la plataforma. Esta posibilidad es tremendamente importante en el caso de sistemas críticos (el sistema de *billing*, el CRM...) en los que no es factible introducir múltiples agentes por su impacto dentro de la funcionalidad del sistema.

Igualmente, los agentes de los sistemas pueden ser utilizados dentro de la infraestructura de seguridad aunque no hayan sido diseñados para esta función. Esto permite, por ejemplo, que cuando un sistema de detección de intrusos detecta un ataque a un sistema (Y) desde otro (X), la plataforma de gestión utilice al agente residente en X para distintos fines: desactivar el usuario que realiza el ataque, parar el sistema para su inspección por el personal de seguridad, etc. El hecho de no utilizar un sistema de detección de intrusos específico significa, además, que el intruso puede que no lo busque activamente para desactivarlo.

De hecho, los agentes de sistemas incluyen entre sus servicios básicos de monitorización algunos servicios relacionados con la seguridad como puede ser el análisis de *logs* para determinar las conexiones de usuarios remotos o los intentos fallidos de conexión. La evolución que ya se está dando en las arquitecturas de agentes de gestión será la integración de todos los agentes de gestión (de seguridad, de gestión del sistema, de gestión SNMP...) en un solo agente con sus sub-agentes específicos. Ofreciendo una plataforma más robusta para su instalación, gestión y despliegue. (ver **Figura 2**)

COOPERACIÓN GESTIÓN DE RED Y GESTIÓN DE SEGURIDAD

Algunas organizaciones desearán utilizar, desde el primer momento, una herramienta de gestión de seguridad. Tanto más cuando su herramienta de gestión de red y sistemas no ofrezca las funcionalidades de correlación de eventos como las de los productos de gestión de seguridad o cuando no se desee realizar el desarrollo específico porque la herramienta seleccionada cubre sus necesidades.

En este caso, la instalación de una nueva consola para los operadores de seguridad no tiene por qué suponer que se tienen dos compartimientos "estancos"

Figura 3: Integración de herramientas de gestión

de información: por un lado los eventos de los sistemas de gestión tradicionales, y por otro los eventos de los sistemas de gestión de seguridad. Habitualmente se configurarán sólo los dispositivos de seguridad (cortafuegos, detectores de intrusos, antivirus...) para enviar sus eventos a la estación de gestión de seguridad y los demás dispositivos (*routers*, *switches*, etc.) enviarán sus eventos a los sistemas de gestión.

La integración entre ambos sistemas de gestión es importante, y supone el reenvío de alarmas relevantes de una estación de gestión a otra. De esta forma se pueden correlacionar eventos significativos pero generados por dispositivos no gestionados directamente. Este intercambio de información permite huir de situaciones de conflicto. Tal sería el caso, por ejemplo, de un ataque con éxito sobre un servidor de DNS mediante una sobrecarga de 'búfer'. Habitualmente se tendrían dos alertas: por un lado la del detector de intrusos en la red del DNS (o un sensor de *host*), que avisaría del ataque, y por otro el del sistema de gestión (que quizá disponga de un agente específico en dicho sistema o realice una monitorización activa remota), que indica que el servicio no está disponible. Si no se intercambia información entre las consolas se daría el caso de que el operador de gestión podría tomar medidas para reactivar el servicio (como entrar en el sistema vulnerado y reactivarlo). Medidas que pueden entrar en conflicto con las actividades realizadas por el operador de seguridad para contener y controlar el problema de seguridad detectado. (ver **Figura 3**)

CONCLUSIONES

Como se ha visto a lo largo del artículo, la gran mayoría los sistemas de gestión ya instalados en las organizaciones pueden convertirse en sistemas de gestión de seguridad gracias a su gran flexibilidad a través de un proceso de definición y adaptación. Asimismo, los propios fabricantes están aprovechando el tirón de la "Seguridad Gestionada" para mejorar las soluciones de seguridad sobre sus propias plataformas, lo cual puede suponer (a largo plazo o a corto según el fabricante) un mejor aprovechamiento de la inversión en infraestructuras, sistemas y aplicaciones ya realizadas por las organizaciones.

La adquisición de una herramienta de gestión de seguridad específica estará justificada en algunos casos, pudiendo ofrecer soluciones *out of the box* a los problemas de una organización. Pero aún en este caso, es necesario que se logre una interoperabilidad entre las distintas herramientas para evitar la *"compartimentalización"* de la información, que puede dar lugar a visiones parciales e incompletas y a inconsistencias en la actuación frente a problemas de seguridad de las organizaciones.

No se puede olvidar, sin embargo, que la gestión de la seguridad, expresión rimbombante con la que muchos fabricantes marcan sus productos, es un problema que no estará nunca totalmente resuelto por las herramientas, ya que éstas, sin personal cualificado o procedimientos específicos, pierden su valor. El hecho es que la evolución en este campo promete grandes cambios en el horizonte, cambios que obligarán a que todos los que participan de la seguridad en las organizaciones se adapten y renueven (empezando por los propios fabricantes y terminando por las propias compañías). Aunque el tiempo lo dirá, es más que probable que las soluciones de gestión ofrecidas por "los grandes" acaben absorbiendo la gestión de seguridad como un elemento más y veremos como las plataformas diseñadas por distintas compañías (algunas de ellas *start-ups* muy recientes) se acabarán incluyendo dentro de soluciones más genéricas y globales. n

PLATAFORMAS DE GESTIÓN DE RED Y SISTEMAS

Plataforma	Compañía	Productos de gestión de seguridad asociados
HP Openview	HP	En desarrollo su integración en HP Openview Operations www.openview.hp.com/products/
Netcool	Micromuse	Netcool for Security Management www.micromuse.com/products/nfsm_def.html
Patrol	BMC	Control-SA – www.bmc.com/security
Spectrum	Aprisma	Spectrum Security Manager – www.aprisma.com/products/security.shtml
Tivoli	IBM	Risk Manager, Intrusion Manager – www.tivoli.com/security

PLATAFORMAS DE GESTIÓN DE SEGURIDAD

Plataforma	Compañía
ActiveEnvoy	NetForensics – www.netforensics.com
e-Sentinel	eSecurity – www.esecurityinc.com
Security Command Center	eTrust – www.cai.com
SecurityManager	NetIQ – www.netiq.com
Solsoft NP	Solsoft– www.solsoft.com
SystemWatch	Open– www.open.com
VigilEnt	Pentasafe* (adquirida en septiembre por NetIQ) – www.pentasafe.com

JAVIER FERNÁNDEZ-SANGUINO PEÑA
jfernandez@germinus.com
ANTONIO REQUEJO NOVELLA
arequejo@germinus.com
División de Seguridad Lógica
GERMINUS SOLUTIONS