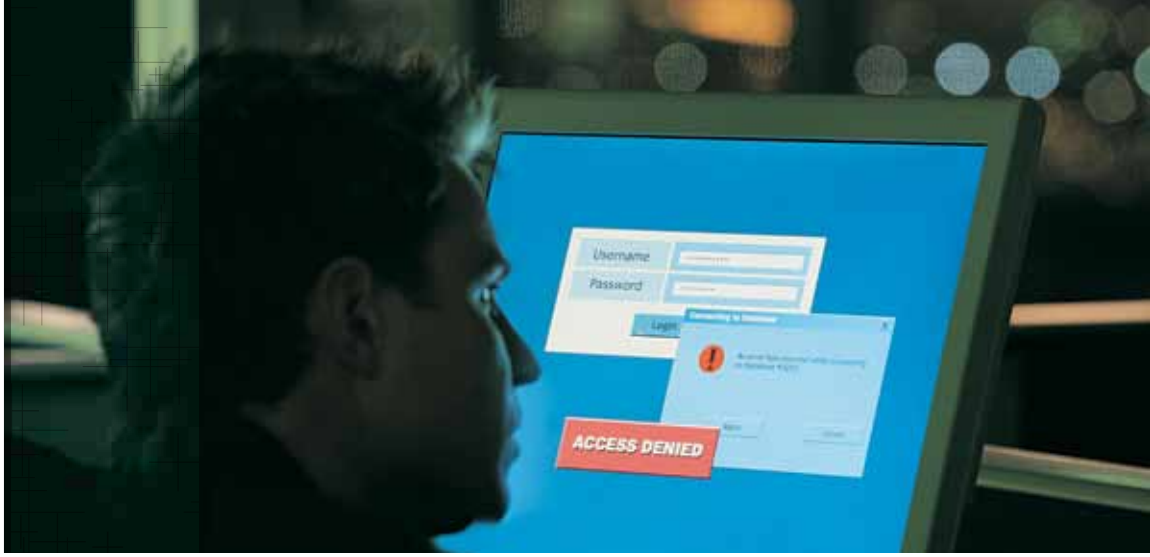
McAfee
An Intel Company

GESTIÓN DE RIESGOS Y SEGURIDAD

Guía de la solución



Security Connected

La plataforma Security Connected de McAfee permite integrar distintos productos, servicios y asociaciones con el fin de reducir los riesgos de forma efectiva, eficiente y centralizada. Sobre la base de más de dos décadas de prácticas de seguridad de eficacia probada, el enfoque de Security Connected ayuda a las organizaciones de todos los tamaños y segmentos, en todas las zonas del mundo, a mejorar el estado de su seguridad, optimizar la protección para mejorar la rentabilidad y alinear estratégicamente la seguridad con las iniciativas empresariales. La arquitectura de referencia de Security Connected le facilita el paso de las ideas a la implantación. Utilícela para adaptar los conceptos de Security Connected a sus riesgos, su infraestructura y sus objetivos empresariales concretos. En McAfee dedicamos todos nuestros esfuerzos a la búsqueda constante de nuevas soluciones y servicios que garanticen la total seguridad de nuestros clientes.

Descargue los últimos recursos en www.mcafee.com/es/enterprise/reference-architecture/index.aspx.

Adopte un enfoque proactivo de la gestión de riesgos

Desafíos

Hasta no hace mucho tiempo, la gestión de los riesgos y de la seguridad se limitaba principalmente a los riesgos financieros y al cumplimiento de normativas. Las auditorías y los procesos de administración eran eventos previsibles, que los departamentos de TI intentaban minimizar y automatizar. El concepto de riesgo era relativamente estático. Sin embargo, en la actualidad, los ataques se han diversificado (discretos y lentos, en el caso de los ataques selectivos, o fulminantes, en el caso de las acciones de ciberactivismo y de los brotes de malware) y su ritmo exige que los equipos de dirección y los administradores de TI presten más atención a los eventos emergentes y tomen decisiones rápidamente basadas en la evaluación de los riesgos para su neutralización.

Y, claro está, la noción de riesgo financiero y de cumplimiento de normativas también es ahora más dinámica. Tengamos en cuenta que, debido al cambio constante de las oportunidades comerciales con la evolución de la economía, los organismos reguladores deben ajustar, de manera independiente, más de 200 directivas en todo el mundo. Ese panorama de riesgos que en su día era estático, en la actualidad fluctúa como un caleidoscopio.

Administrar grandes volúmenes de datos de seguridad

En la actualidad, la gestión de los riesgos implica dar sentido a un número cada vez mayor de datos: análisis de vulnerabilidades, registros de aplicaciones y bases de datos, flujos, registros de sesiones y de acceso, alertas y análisis de tendencias. Los flujos de datos proceden de una gran cantidad de sistemas encargados de proteger a un número cada vez mayor de usuarios, que acceden desde más ubicaciones a través de más dispositivos.

Las auditorías (motivadas por directrices internas o externas) ilustran claramente la dificultad de administrar los datos recopilados de una enorme cantidad de fuentes. Los administradores de TI deben identificar y recopilar flujos de datos en el formato exigido por los auditores. Las auditorías, por definición, analizan una situación anterior y evalúan los riesgos pasados. Socavan los recursos de la empresa y desvían su atención de una prioridad más importante: la gestión proactiva de riesgos, es decir, la capacidad de anticipar, comprender y limitar los riesgos, que están en constante evolución, antes de que causen daños.

Evaluar los riegos

El mundo entero se enfrenta al fenómeno de la explosión de los volúmenes de datos y, en el ámbito que nos ocupa, de grandes volúmenes de datos de seguridad. Comprender todos los matices de las amenazas de seguridad puede llevar días, o incluso meses. La mayoría de los analistas de seguridad se enfrentan a problemas de gestión de los datos similares a los de los administradores de TI encargados de las auditorías: esa ingente cantidad de flujos de datos aislados complica mucho la tarea de confeccionar una imagen concisa y coherente de los eventos. Cuanto mayor es el volumen de datos recopilados y analizados, más complicado resulta ordenar y reconstruir los eventos. Es necesario esperar a disponer de una imagen precisa de la situación (es decir, mucho tiempo después del evento) para adaptar las directivas y los sistemas de protección con el fin de evitar que vuelva a repetirse.

¿Qué ocurre si el ataque es brutal y rápido, por ejemplo, un ataque de denegación de servicio o un gusano de propagación rápida? Si se necesitan días o meses para diagnosticar el problema, las repercusiones para la empresa podrían ser tremendas (o incluso fatales) desde el punto de vista financiero y de cumplimiento de normativas. ¿Qué activos son realmente vulnerables a esta amenaza y cuáles disponen de controles o de contramedidas para neutralizarla? Para responder a esta pregunta, los administradores necesitan disponer de visibilidad sobre el nivel de seguridad del conjunto de sistemas, incluido el arsenal, cada vez mayor, de dispositivos móviles y personales que acceden a sus redes.

Reaccionar ante los eventos

Tras comprender correctamente la amenaza, es necesario establecer las prioridades y aplicar las medidas correctivas. ¿Cuáles son los activos más importantes? ¿Cuáles pueden esperar? Los administradores cambian con frecuencia de consola de administración para realizar análisis, ejecutar secuencias de comandos, ajustar directivas, instalar actualizaciones o poner en cuarentena los sistemas. Todos estos productos que inundan el mercado de la seguridad no hacen sino aumentar el coste y la complejidad, debido a la diversidad de interfaces de usuario, formatos de datos, estándares de directivas o tipos de informes. Esto se traduce inevitablemente en errores y en lagunas en la cobertura, que exponen a la empresa y a sus activos a riesgos innecesarios (y, generalmente, mal identificados).

Ya no basta con actuar de forma reactiva en lo relativo a la gestión de riesgos. Debe anticiparse, con una visión completa de la situación, para identificar y gestionar los riesgos a medida que cambian. La información sobre cada situación específica frente a los riesgos proporciona un contexto dinámico sobre el entorno de amenazas global, así como sobre los activos y el nivel de seguridad de su empresa. Las tecnologías de gestión de riesgos automatizadas utilizan este contexto para ayudarle a conocer las relaciones entre los diferentes elementos, con el fin de que pueda optimizar las directivas y las protecciones.

Soluciones

Los grandes volúmenes de datos de seguridad y los problemas que generan a nivel de procesos operativos complican la gestión de los riesgos y la seguridad, pero el empleo de una estrategia global unida a tecnologías modernas puede ayudar a poner orden en todo este caos. En el contexto de los procesos de gestión de riesgos financieros y del cumplimiento de normativas, necesita considerar, en tiempo real, los riesgos potenciales que plantean los eventos internos y externos. Un enfoque unificado permite simplificar los procesos y dar respuestas automatizadas que reducen los costes y el tiempo de respuesta. Los equipos de dirección consiguen visibilidad del impacto de los eventos de seguridad en el estado de riesgo, mientras que los administradores disponen de la información y el control necesarios para limitar los riesgos de forma proactiva.

Los sistemas de administración de eventos e información de seguridad (SIEM) modernos están estrechamente integrados con la administración de la seguridad y del cumplimiento de normativas de dispositivos, servidores, redes, aplicaciones y bases de datos. Esta plataforma de administración de la seguridad puede proporcionar un control que facilita la visibilidad y la agilidad operativa. Cuanto más estrecha sea la integración entre estos sistemas, la información sobre riesgos y los sistemas de seguridad, más fácil le resultará comprender y gestionar los riesgos. Un enfoque basado en una plataforma armoniza y unifica los procesos, las directivas, los flujos de trabajo y los informes individuales y fragmentados. La incorporación de información actualizada permite analizar los datos en función de la evolución de los riesgos y contribuye a mejorar la precisión, la pertinencia y el tiempo de respuesta para limitar el riesgo.

Evaluar las vulnerabilidades

La mayoría de las entidades sometidas a normativas analizan las vulnerabilidades con el fin de respetar los imperativos de cumplimiento de normativas. Sin embargo, los análisis planificados olvidan sistemáticamente los sistemas remotos y los inactivos, o bien ignoran activos estratégicos de la empresa, como las aplicaciones y las bases de datos. Los sistemas no fiables pueden, de esta forma, pasar desapercibidos y albergar vulnerabilidades aprovechables. Un método más riguroso para administrar las vulnerabilidades en activos de red puede tener en cuenta estos sistemas diversos y eliminar los los vacíos en el cumplimiento de normativas. Puede utilizar la información dinámica sobre riesgos, el valor de los activos y las contramedidas apropiadas para llevar a cabo análisis o para implementar controles de compensación.

Mejorar el conocimiento de la situación

A la vista de los ciberataques y de la permeabilidad de los perímetros, la mayoría de las empresas desean comprender y responder mejor a los riesgos en constante evolución. La clave es identificar los que son realmente importantes, en el momento oportuno. Si disponen de la velocidad y la capacidad necesarias para gestionar grandes volúmenes de datos, las herramientas SIEM pueden supervisar las aplicaciones y las bases de datos, administrar los registros y normalizar los eventos en paneles de datos correlacionados. Algunas integran además conocimientos en tiempo real del panorama de amenazas, así como de usuarios, sistemas, datos, riesgos y contramedidas. Gracias a esta completa imagen del contexto situacional, puede comprender rápidamente la actividad relacionada con la seguridad, incluida la actividad histórica. Mediante el uso de herramientas analíticas robustas puede pronosticar e identificar los ataques, así como neutralizar las amenazas en minutos, en lugar de en horas.

Inspeccionar el tráfico de red

Las redes representan al mismo tiempo la infraestructura crítica y las vías por las que pueden filtrarse datos confidenciales y sometidos a normativas. La supervisión y administración del tráfico de red, incluido el tráfico cifrado, permiten a los administradores reducir el uso no apropiado o peligroso de Internet y de las aplicaciones, y garantizar la implementación de las directivas de contenido. La integración de soluciones de seguridad para redes de próxima generación con sistemas SIEM y de protección seguridad de sistemas ayuda a los gestores de riesgos a implementar directivas, proteger contra la amenazas de tipo zero-day, así como a supervisar, analizar e informar sobre el cumplimiento de normativas.

Optimizar la administración de registros

Los registros proporcionan una enorme cantidad de datos que utilizará en la administración de las pruebas electrónicas, las auditorías y para el proceso de cumplimiento de normativas, siempre y cuando sea capaz de ordenar los datos recopilados para extraer la información relevante. Gracias a una solución de administración de registros integrada, segura y de alto rendimiento, puede recopilar los datos en tiempo real de todas las fuentes pertinentes y conservar los registros conforme a un procedimiento normalizado y protegido de la cadena de custodia. El control de las aplicaciones puede evitar que los ciberdelincuentes pirateen los sistemas de registro para ocultar sus acciones. La asociación de funciones de administración de registros y otras herramientas analíticas de los riesgos y de la seguridad permite transmitir los datos de registros a los usuarios que mejor pueden utilizarlos para gestionar los riesgos.

Consideraciones sobre buenas prácticas

- Alinear y unificar los procesos y controles fragmentados
- Automatizar la recopilación, la correlación, la evaluación, la respuesta y la supervisión
- Aprovechar información dinámica sobre los riesgos, análisis hipotéticos y respuestas basadas en directivas para identificar y bloquear las amenazas de forma proactiva
- Garantizar que los programas de gestión de riesgos y seguridad cubren todos los dispositivos, todos los datos y toda la infraestructura de TI
- Reunir toda la información sobre riesgos y seguridad de toda la empresa en una misma plataforma para optimizar la gestión
- Supervisar la situación de forma constante y proactiva para detectar y responder a los riesgos en constante evolución, mantener el cumplimiento de normativas y prevenir eventos de seguridad futuros

Los procesos manuales de gestión de riesgos y seguridad tienen una probabilidad mayor de generar errores y constituyen uno de los principales factores del incremento de los costes de la seguridad y del cumplimiento de las normativas.

Generación de valor añadido

Una estrategia de gestión de riesgos y de seguridad global que se apoya en una plataforma de administración automatizada y con gestión de riesgos aportará una gran cantidad de ventajas para su empresa:

- Conocimiento de la situación a través de detallada información de contexto y de análisis completos
- Diagnóstico de incidentes y reacción en cuestión de segundos, no de horas, para limitar los daños, impedir las fugas de datos y reducir los costes de la aplicación de medidas correctivas
- Disminución del número de incidentes de seguridad, de infracciones de cumplimiento de normativas y de los costes por incidente
- Simplificación de los procesos de configuración de directivas de cumplimiento de normativas y de generación de informes para mejorar la eficacia operativa
- Disminución del número de plataformas, hardware y software de proveedores utilizados para administrar la seguridad
- Reducción de los costes operativos y del tiempo dedicado a la formación

Material relacionado de la arquitectura de referencia Security Connected

Nivel II
- Control y supervisión de cambios
- Protección del centro de datos
- Conformidad con PCI

Nivel III
- Evaluación de vulnerabilidades
- Mejora del conocimiento de la situación
- Inspección del tráfico de red
- Optimización de la administración de registros
- Investigación de las fugas de datos
- Integración segura de los medios sociales
- Protección de la propiedad intelectual

Para obtener más información acerca de la arquitectura de referencia de Security Connected, visite: www.mcafee.com/es/enterprise/reference-architecture/index.aspx.

Acerca del autor

Barbara G. Kay es analista principal en Secure By Design Group y posee la certificación CISSP. Está especializada en protección de la información para empresas distribuidas y móviles, así como en sensibilización de los internautas para un uso seguro de Internet. Antes de crear Secure By Design en 2006, Barbara fue directora de marketing del proyecto SPI (Security and Privacy Initiative) de Sun. Es licenciada por el Darthmouth College.

McAfee, S.A.
Avenida de Bruselas nº 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8535
www.mcafee.com/es