McAfee®
An Intel Company

SECURITY CONNECTED: OPTIMICE SUS NEGOCIOS

Los 10 principales temas de seguridad que todo ejecutivo debería conocer

10

SECURITY CONNECTED REFERENCE ARCHITECTURE

LEVEL **1** 2 3 4 5

Categorías de ataque:

1. Ataques oportunistas
2. Ataques dirigidos

Tendencias:

3. Protección de los entornos virtualizados
4. Habilitando la "consumerización" de la TI
5. Aprovechando las tecnologías de la nube con seguridad
6. Facilitando la Web 2.0 segura
7. Protección de la información
8. Cómo proteger el moderno *Centro de datos*

Prioridades:

9. El alineamiento de la seguridad como un habilitador de negocios
10. Reduciendo la complejidad y el caos mientras alcanza la conectividad

INTRODUCCIÓN
Los 10 temas principales

Las organizaciones están evolucionando de una manera rápida y constante. Según un reciente informe de Gartner, los CIO están haciendo la transición desde la gestión de los recursos hacia la demostración del valor en términos de negocio. La Encuesta *Agenda del CIO 2011* de Gartner señaló que para el año 2014, los CIO dicen que su enfoque se moverá de la mejora de los procesos y de la reducción de los costos de la empresa hacia el crecimiento empresarial, la mejora de las operaciones y mantener nuevos clientes. Apoyar y habilitar a los negocios y la seguridad debe ser un componente integral de la estrategia general de TI de un CIO.

Paralelamente, el escenario de amenazas está cambiando más rápido que aquello que la mayoría de las organizaciones de TI es capaz de enfrentar. El delicado equilibrio de tornar viables los negocios y mantenerlos protegidos exige que los ejecutivos se mantengan informados sobre esos cambios para que puedan tenerlos en cuenta al tomar sus decisiones. Hemos creado esta guía para educar e informar. Está basada en comentarios de los clientes de McAfee en organizaciones públicas y privadas de todo el mundo. Este no es un análisis exhaustivo de cada uno de los 10 temas, sino más bien presenta una breve sinopsis de los mismos, varios casos de uso, conceptos clave y las referencias a nuestra arquitectura Security Connected, que proporcionan detalles sobre las soluciones, los módulos de tecnología, las mejores prácticas y guías de implementación.

El enfoque Security Connected de McAfee es una estructura para integrar varios productos, servicios y sociedades y proporcionar una reducción centralizada, eficiente y eficaz de mitigación de los riesgos. Con más de dos décadas de experiencia, seguimos ayudando a las organizaciones de todos los tamaños, todos los segmentos y en todas las regiones geográficas a elevar su nivel de seguridad, optimizar la seguridad para lograr mayor eficacia económica y alinear estratégicamente la seguridad con las iniciativas empresariales. El enfoque Security Connected de McAfee proporciona la seguridad que ofrece protección en todas partes a su infraestructura de TI.

1 AMENAZAS
Ataques oportunistas

La nueva escuela del malware y de los bots está muy centrada en las aplicaciones. Para comprender la gravedad de la situación, considere el Facebook, con más de 350.000 aplicaciones, los iPhones de Apple, con más de 100.000, y la introducción del HTML 5 como un vehículo para hacer que la línea entre las aplicaciones locales y remotas sea cada vez más indistinta.

En el siglo diecinueve, la Revolución Industrial aceleró y avanzó los métodos de montaje desde la producción individual hacia la producción masiva. Igualmente, los ciberdelincuentes han madurado y ya utilizan la automatización para desarrollar ataques virtuales más sofisticados y rentables (o "hacking") con mayor agilidad. Dichos ataques oportunistas son organizados y casi siempre tienen una motivación financiera. En muchos casos, los grupos que crean dichos ataques llevan más de una década de experiencia, relaciones delictivas de largo plazo y redes de confianza. Sus funciones se han especializado para promover la escalabilidad. Algunos ejemplos de estas funciones especializadas incluyen cardadores, desarrolladores de *malware* y de *botnets*, distribuidores de *spam*, lavado de dinero y falsificadores de documentos.

Muchos de los bots oportunistas intentan robar datos tales como información de tarjetas de crédito o información de identificación personal. Si no existe nada valioso en el sistema atacado, la víctima se convertirá por lo menos en un integrante inconsciente del "rebaño" de *botnets* y resultará usado para distribuir más *malware*, *spam* y ataques distribuidos de denegación de servicio (DDoS). Para aumentar el alcance, el anonimato, la eficiencia y la eficacia, muchos de esos invasores usan robots para penetrar en los mecanismos de búsqueda para que las búsquedas más frecuentes generen páginas malintencionadas presentadas a los usuarios incautos. A ello se le llama "optimización criminal de mecanismos de búsqueda". Por ejemplo, las cinco búsquedas por celebridades más peligrosas de 2010, con una probabilidad mayor de resultar en *malware* que vulnera los navegadores de la Web y aplicaciones semejantes, son: Cameron Díaz, Julia Roberts, Jessica Biel, Gisele Bündchen y Brad Pitt. No importa si es un individuo o una organización multinacional: si existen recursos *online*, resultarán atacados. No es nada personal, sino tan solo negocios.

Ejemplos de uso	Conceptos principales
• *Spear-phishing* y *spam*	• La mayoría de los ataques oportunistas que buscan obtener ganancias
• Distribución de *malware*	• Los bots poseen un ancho de banda y recursos de procesamiento aparentemente ilimitados Por ejemplo, el *malware* "Conficker" infectó a de 6,4 millones de sistemas en 230 países con una capacidad de procesamiento total y ancho de banda mayores que Amazon y Google juntos
• Interrupción de servicio por DDoS	• Los atacantes han tenido más de una década para madurar su modelo de negocios, desarrollar redes confiables y crear la especialización de las competencias
Arquitectura de Referencia Security Connected Nivel 2 – Temas por considerar	
• Protección de la información	
• Protección del Centro de datos	

2 AMENAZAS
Ataques dirigidos

Los ataques dirigidos resultaron en la censura de los medios, la bancarrota de empresas, el robo de miles de millones de dólares en propiedad intelectual y campañas militares que combinaron técnicas de guerra estáticas y de movimiento para lograr una ventaja táctica.

Los ataques dirigidos han asumido muchas formas diferentes que son altamente automatizadas, discretas y lentas, aprovechando la manipulación de dispositivos para obtener acceso o información y combinando componentes de ingeniería social. Los autores de este tipo de ataques tienen una misión. Aunque los ataques dirigidos abarquen mucho más que el sabotaje o la vigilancia, están frecuentemente asociados al espionaje, y, así, el concepto es anterior a la era digital, llegando a los primeros documentos de recopilación de información registrados por estrategas militares como Sun-Tzu y Chanakya. Los ataques dirigidos han recibido una gran cobertura mediática. Esto se debe, en parte, a una serie de ataques cibernéticos denominados Operación Aurora, Night Dragon, Shady Rat, y Stuxnet. Estos ataques dirigidos, aunque no siempre fueron muy sofisticados, eran centrados, sigilosos y diseñados para la manipulación a largo plazo de sus objetivos. Los ataques dirigidos solo tienen que ser tan avanzados como lo requiera su objetivo; en muchos casos, los ataques de spear *phishing* e inyección de SQL actúan como vectores de ataque.

Ejemplos de uso	Conceptos principales
• Robo de secretos comerciales	• Los ataques dirigidos son más a menudo impulsados por la economía o la política
• Robo de secretos del gobierno	• Detrás de los ataques hay atacantes motivados y con frecuencia bien financiados, usualmente asociados a estados nacionales y/o a quienes los apoyan, competidores, el crimen organizado, activistas y, posiblemente, terroristas
• Sabotaje de activos de infraestructura crítica	• Buscan mantener el camuflaje y el acceso por períodos de tiempo prolongados
Arquitectura de Referencia Security Connected Nivel 2 – Temas por considerar	
• Protección de la información	
• Protección del Centro de datos	

3 TENDENCIAS
Protección de los entornos virtualizados

En el inicio, Popek y Goldberg definían una máquina virtual como "un método eficaz y aislado de duplicar una máquina real". Ello incluía fallas de seguridad y todo el resto. La virtualización no certifica una seguridad similar.

La virtualización y las máquinas virtuales (VM) se convirtieron en una fuerza de la industria. Existen algunos proveedores principales de *desktops* y servidores virtualizados, y otros están ingresando en el mercado para solucionar retos específicos creados por los entornos virtuales. Además, muchas empresas están empezando a buscar servicios de virtualización provistos a través de la nube. Las fuerzas resultantes de la virtualización son la reducción de los costos de hardware, la mejora de la administración del sistema y la reducción del consumo de energía (el "green computing", reducción del espacio físico y otras ventajas). Aunque la virtualización sea todavía una tecnología relativamente nueva, muchos sectores la están adoptando ampliamente. Los beneficios de negocios de esas nuevas plataformas muchas veces sobrepasan y preocupan a los profesionales de seguridad. Sin embargo, hay una percepción errónea de que una solución, porque está virtualizada, es segura, y esto simplemente no es verdad. Y, hay otra idea errónea de que la adición de capas de seguridad reducirá la velocidad/capacidad disponibles en los entornos virtualizados. La maniobra es la siguiente: las mismas consideraciones que se aplican a los sistemas físicos se deben aplicar a los virtuales, sin dejar de tener en cuenta las adaptaciones del entorno operativo.

Ejemplos de uso	Conceptos principales
• Proteger las VM, ya sea *online* u *offline*	• Las VM son dinámicas; se activan y desactivan y, a menudo, se transfieren, dificultando la estandarización de la seguridad
• Proteger los hipervisores contra ataques	• Se atacarán a los hipervisores al igual que cualquier sistema operativo común, pero las amenazas también pueden llegar a través de las consolas de las soluciones de virtualización y aplicaciones de gestión
• Proteger las máquinas virtuales invitadas contra los ataques; otras máquinas virtuales o sistemas externos	• Se puede conseguir la seguridad de las máquinas virtuales sin obstaculizar la eficacia operativa de la virtualización
Arquitectura de Referencia Security Connected Nivel 2 – Temas por considerar	
• Protección de dispositivos móviles	
• Permitir la "consumerización" de los empleados	

4 TENDENCIAS
Habilitando la "consumerización" de la TI

"La electrónica del consumidor afectará a todas las empresas", afirmó David Mitchell Smith, Vicepresidente y Asociado de Gartner. "Los intentos de las empresas de negarlo están sujetos al fracaso, como han fracasado los intentos anteriores de negar la WiFi, los teléfonos celulares 'inteligentes', Internet, incluso las PC".

Imagínese una oficina sin acceso a Internet, *email*, la Web, ni a computadoras. Imagínese no tener impresoras ni teléfonos. La mayoría de las empresas simplemente no serían capaces de operar. Con el avance de la tecnología y la reducción de costos, las personas se están dando cuenta de que sus soluciones personales de tecnología, que aparecen en primer lugar en el mercado consumidor, son suficientemente potentes y versátiles para el uso profesional. En muchos casos, son aún más potentes y su costo es menor. Por lo cual, la división entre la TI y los dispositivos electrónicos de consumo que los empleados creen que necesitan para trabajar se volvió imprecisa. Ello resultó en un crecimiento explosivo del uso de la tecnología personal en el mundo profesional: portátiles, tabletas, *smartphones*, reproductores de MP3 y dispositivos de almacenamiento USB. Una pregunta muy usual es: "¿Cómo podemos proteger nuestro patrimonio y nuestra propiedad intelectual si los empleados conectan sus dispositivos personales?"

Ejemplos de uso	Conceptos principales
• Proporcionar flexibilidad a los empleados y, al mismo tiempo, reducir los riesgos para la empresa	• Los teléfonos inteligentes llegaron para quedarse, y esté preparado para admitir muchos tipos más de dispositivos y tabletas. En 2010, se introdujeron más de 35 tipos diferentes de tabletas en el mercado, y su rápida tasa de adopción en las empresas resulta evidente en los aeropuertos y en las oficinas de todo el mundo.
• Aprovechar la capacidad que la electrónica de consumo puede llevar al lugar de trabajo	• Los usuarios citan la gran eficacia de la tecnología de consumo y su capacidad de trabajar con más facilidad
• Proteger los datos confidenciales en dispositivos móviles, especialmente los *smartphones*	• Aunque la "consumerización" de la TI sea un concepto relativamente nuevo, ya existen controles de seguridad para atenuar los riesgos vinculados a los dispositivos de consumo

Arquitectura de Referencia Security Connected Nivel 2 – Temas por considerar
• Protección de dispositivos móviles
• Permitir la "consumerización" de los empleados

5 TENDENCIAS
Aprovechando las tecnologías de la nube con seguridad

El cómputo en la nube es uno de los segmentos que más crecen en la tecnología de la información. Las empresas de todos los tamaños buscan el cómputo en la nube como una forma de aumentar la agilidad comercial y disminuir sus costos. Las organizaciones resultan atraídas por la perspectiva de acelerar su capacidad de usar aplicaciones de negocios, como *email* y administración de relación con los clientes (CRM), o de aprovechar una infraestructura interna con más recursos, a un costo reducido. La nube, sin embargo, ha enfrentado algunas vulnerabilidades de seguridad y fallas de servicio, tales como: la indisponibilidad del Google App Engine, las interrupciones del Gmail, fallos de dispositivos de red que impidieron el acceso de miles de personas a las aplicaciones de software como un servicio (SaaS) de Salesforce.com, y otros problemas semejantes con Apple, Yahoo y Amazon.

Dos importantes obstáculos para la adopción de la nube en las 1500 empresas encuestadas en el estudio de Cloud Computing en las Empresas realizado por IDG en noviembre de 2010, fueron los siguientes:

- *Seguridad: un 67 % citaron como una preocupación, el riesgo de acceso no autorizado, la capacidad de mantener la integridad de los datos y la protección de los datos*
- *Acceso a la información: un 41% estaban preocupados por la posibilidad de ser capaces de preservar privilegios uniformes de acceso en las aplicaciones de la nube*

Ejemplos de uso	Conceptos principales
• Adopción del SaaS	• Identificar dónde residen sus datos, qué sistemas ocupa como parte de la prestación de servicios, y dónde son almacenados y archivados
• Usar un centro de datos subcontratado o una infraestructura como un servicio	• Saber quién tendrá derechos de administración física y lógica en las situaciones de producción y conmutación por error (*failover*)
• Extender el Centro de datos convencional	• Entender cómo se debe monitorear la red, los sistemas y los recursos de datos
Arquitectura de Referencia Security Connected Nivel 2 – Temas por considerar	
• Cómo proteger el Centro de datos	
• Proteger las aplicaciones de la nube	

6 TENDENCIAS
Facilitando la Web 2.0 segura

Internet es la primera cosa que la humanidad construyó y no comprendió; fue la mayor experiencia anarquista de todos los tiempos".

—Eric E. Schmidt
Presidente de la Junta
y CEO de Google

Facebook es el sitio más popular de Internet, y otras redes sociales y soluciones de la Web 2.0 no se quedan muy rezagadas. Empresas de todos los tamaños están encontrando nuevos rumbos para comercializar o nuevas formas de expandir sus negocios usando las aplicaciones de la Web. Los empleados y las empresas están usando los recursos de la Web 2.0 para uso personal y de negocios. Ello no es muy distinto a los inicios del *email* y de los navegadores de la Web. Bloquear el acceso es, a lo sumo, una solución temporal. Al fin y al cabo, las personas tendrán que acceder y/o encontrar formas de esquivar los controles. Las organizaciones deben establecer un equilibrio entre una mano de obra eficaz y ágil y controles y políticas de seguridad eficaces. Quizás las soluciones de seguridad existentes no sean capaces de resolver el problema; administrarlo con varios proveedores puede ser extremamente complejo, exige esfuerzo manual y es propenso a errores. Puede ser difícil atraer y mantener a los empleados si las políticas son muy rigurosas.

Se pueden perder oportunidades de negocios debido a un enfoque excesivamente cauteloso. Pero la falta de controles de seguridad puede exponer individuos y empresas a amenazas como el *malware*.

Ejemplos de uso	Conceptos principales
• Controlar el acceso, las descargas y las publicaciones	• Las soluciones de la Web 2.0 se están volviendo tan comunes e importantes como el *email* y los navegadores de Web
• Ser suficientemente ágil para permitir que los empleados, clientes y socios aprovechen con seguridad las soluciones de la Web 2.0	• Bloquear el uso de la Web 2.0 es, a lo sumo, una solución a corto plazo

Arquitectura de Referencia Security Connected Nivel 2 – Temas por considerar
• Permitir el uso seguro de los medios sociales
• Permitir la "consumerización" de los empleados

7 TENDENCIAS
Protección de la información

"La vida se resume a administrar los riesgos, y no a eliminarlos".

—Walter Wriston
Ex presidente y CEO
de Citicorp

La protección de datos se ha convertido en uno de los aspectos más importantes de una eficaz estrategia de seguridad. Información reglamentada vinculada a registros financieros, registros médicos y datos confidenciales son sumamente valiosos. Es el objeto de deseo de integrantes de las empresas, intrusos oportunistas y ataques dirigidos con motivación financiera o política. Los controles tradicionales de seguridad de red por si solos no ofrecen una protección adecuada; se necesitan soluciones dedicadas capaces de proteger datos estáticos, móviles y en uso. Dichas soluciones deben abarcar los puntos de transacción tales como aplicaciones y bases de datos, y terminales tales como servidores de archivos, portátiles y dispositivos móviles. Deben también monitorear cómo se accede a dichos datos y el comportamiento de quien los utiliza. Ese monitoreo revela cómo se transportan los datos por la red.

La protección de datos no puede ser eficaz si opera aislada. Reunir la protección de datos en todas las tecnologías de transportes y aplicaciones beneficia a todos. Utilizando dichos controles de una forma coordinada, el conocimiento de la situación se vuelve más real, pues los puntos ciegos que deja un control pueden ser llenados por otro, lo que eleva la postura general de seguridad de la organización. Las organizaciones son capaces de tomar mejores decisiones de una forma más ágil, porque tienen evidencias conocidas de actividades ilegales con los datos y en las redes. La solución adecuada de protección de datos puede generar respuestas rápidas para estas preguntas difíciles:

- ¿Donde están los datos que necesitan protección?
- ¿Quién tiene acceso a ellos?
- ¿Cómo se usan los datos?
- ¿Quién más está involucrado, qué más puede estar ocurriendo, y hace cuanto que está ocurriendo?

Ejemplos de uso	Conceptos principales
• Proteger datos confidenciales contra actividades descuidadas y malintencionadas, sin bloquear el acceso	• Una protección de datos eficaz debe transcender a los datos estáticos, móviles y en uso en todas las aplicaciones y bases de datos, terminales y dispositivos móviles
• Lograr una visión rápida de los riesgos a los datos y a la red, además de demostrar cumplimiento.	• Uno de los resultados más valiosos de reunir controles de datos y de red es la capacidad de comprender totalmente cómo los usuarios interactúan con los datos

Arquitectura de Referencia Security Connected Nivel 2 – Temas por considerar
• Protección de la información
• Cómo proteger el Centro de datos
• Cómo controlar y monitorear los cambios

8 TENDENCIAS
Cómo proteger el moderno *Centro de datos*

"Las cuatro principales razones detrás de los planes de una empresa para actualizar su centro de datos son las siguientes: aumentar la disponibilidad/ el tiempo de operación, reducir los riesgos, flexibilidad para reaccionar a los cambios en las condiciones del mercado, y reforzar la seguridad."

—Encuesta de Network World en nombre de McAfee y Brocade, marzo de 2011

Los centros de datos dirigen las organizaciones. Generar ingresos, almacenar datos confidenciales y proveer servicios esenciales son sólo algunas de sus funciones. Debido a su carácter crítico y a su valor, son de suma importancia. Los datos confidenciales, aplicaciones empresariales, bases de datos, dispositivos de red, almacenamiento, e infraestructura de apoyo, han estado durante mucho tiempo en la mira de los atacantes externos e internos, así como los auditores, armados con las exigencias reglamentarias.

Prácticamente todos los problemas de seguridad en los centros de datos y las leyes han dado lugar a una solución puntual. Este proceso reactivo, donde nuevas soluciones se añaden a cada paso, ha dado como resultado controles de centros de datos que son complejos, costosos, numerosos y desconectados, lo que preocupa a la mayoría de las organizaciones. Además de los requisitos existentes, nuevas amenazas y tendencias entran continuamente en el proceso. Por ejemplo, las organizaciones requieren que sus centros de datos soporten la movilidad y la Web 2.0, proporcionen protección contra los ataques dirigidos y oportunistas, y lo hagan todo mientras reducen al mínimo el tiempo de inactividad y producen informes frecuentes para demostrar el cumplimiento.

La seguridad clásica de los centros de datos carece de la agilidad de hacer negocios para cumplir de una forma rápida y sin obstáculos con los nuevos requisitos; la gestión de la seguridad para fines de eficiencia y eficacia; la disponibilidad e integridad necesaria para las operaciones esenciales de hoy en día; y de un diseño optimizado para la rentabilidad. Los centros de datos han evolucionado y se volvieron más esenciales que nunca. Hoy en día, los departamentos de TI están abriendo nuevos caminos. Podemos especular acerca de la próxima "revolución" de los próximos cinco años, pero si los últimos cinco años son una medida, lo que pensamos que nos brindaba seguridad ya no nos mantendrá seguros. Se necesita un marco estratégico que ayude a conectar las piezas que siempre han estado dispersas.

Ejemplos de uso	Conceptos principales
• Adoptar las tendencias de los centros de datos, incluyendo la consolidación, la virtualización y la nube	• Se debe reducir la complejidad de las operaciones de los centros de datos para lograr la reducción de los riesgos y aumentar los niveles de eficacia
• Proteger los datos confidenciales en el centro de datos y, al mismo tiempo, optimizar las operaciones	• Las arquitecturas de los centros de datos se deben construir sobre un marco flexible que pueda facilitar la adopción de nuevas tendencias, como la "consumerización" de la TI, la informática móvil, los entornos virtuales, y aspectos semejantes – esta flexibilidad permitirá una incorporación más rápida de dichas tendencias con muy poca perturbación, y aumentará al máximo la atenuación de los riesgos

Arquitectura de Referencia Security Connected Nivel 2 – Temas por considerar
• Cómo proteger el Centro de datos
• Administración de la seguridad y del riesgo
• Permitir la "consumerización" de los empleados

9 PRIORIDADES
Alineamiento de la seguridad como habilitador de Negocios

"Raramente las oportunidades tienen rótulos".

—John A. Shedd
Escritor y profesor estadounidense

Hace una década, pensar en la seguridad como un mecanismo para afectar positivamente a las operaciones de negocios, como un diferencial competitivo y permitir nuevas iniciativas de negocios era, como mucho, un debate académico. Sin embargo, las amenazas continúan evolucionando los consumidores y las empresas se volvieron más conscientes de los riesgos y exigen niveles elevados de seguridad.

Los consumidores no están dispuestos a desechar la practicidad ofrecida por Internet, los dispositivos móviles y la Web 2.0. Pero las estadísticas muestran que, ahora, los clientes consideran la seguridad uno de sus criterios al decidir que harán negocios con una organización, y que una violación de datos sería un motivo convincente para que terminar una relación de negocios.

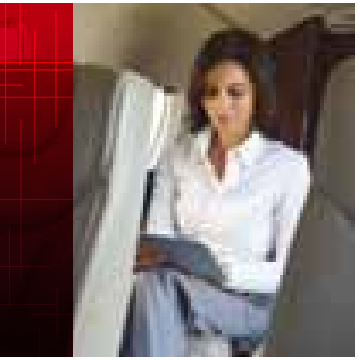
¿Cómo la seguridad promueve los negocios?

- Afecta positivamente a las operaciones de negocios, permitiendo el uso de aplicaciones de negocios *online* sin sacrificar la integridad de los datos o su confidencialidad.
- Actúa como un diferenciador competitivo, permitiendo que los empleados y clientes aprovechen de forma segura las aplicaciones móviles y la Web 2.0 para interactuar con la empresa
- Posibilita nuevas iniciativas de negocios, evitando que los datos confidenciales, tales como información de clientes, lanzamientos de nuevos productos, actividades de fusión y adquisición, y campañas de marketing, fuguen descuidos o actos maltintencionados

Arquitectura de referencia Security Connected Nivel 2 – Temas por considerar
• Protección de dispositivos móviles
• Permitir el uso seguro de los medios sociales
• Proteger las aplicaciones de la nube
• Permitir la " consumerización" de los empleados

10 PRIORIDADES

Reduciendo la complejidad y caos mientras alcanza la conectividad



No hace mucho que era necesario proteger sólo los sistemas de informática fijos en sitios físicos asignados en su empresa. Hoy, usted necesita una seguridad que proteja una red virtual datos, aplicaciones y servicios que pueden estar en cualquier lugar y momento. La seguridad necesita alcanzar la misma ubicuidad. Para alcanzar ese objetivo, quizás el mayor enemigo sea la complejidad. Tener una solución de seguridad por encima de otra en una forma desarticulada solo para solucionar un riesgo específico a la seguridad genera complejidad y, a menudo, hace que la cura sea peor que la enfermedad. El viejo modelo de defensa a profundidad debe ser actualizado. Se requiere un enfoque más reflexivo, que optimice la inversión en la seguridad, y que resulte en la mejora del perfil de riesgo y de la seguridad a un costo reducido.

"Ser sencillo es ser grande".

—Ralph Waldo Emerson
Ensayista y poeta
estadounidense

Durante años, la seguridad viene intentando asumir una función más estratégica dentro de la TI y las operaciones de negocios en general. Ello es virtualmente imposible cuando el procedimiento estándar de operación es el de detectar una amenaza a la seguridad y manejarla como una solución aislada. Ahora, se requiere a los equipos de operaciones para resolver un número cada vez mayor de amenazas con soluciones aisladas utilizando el mismo personal de seguridad (o con menos personas).

Con los expertos en seguridad empujando a las organizaciones a pensar en la seguridad de la red, la seguridad de sistemas, la seguridad de datos y la conformidad como parte de una estrategia unificada, ¿qué pueden hacer las empresas para reducir la complejidad hasta un punto que sea operativamente viable, y no sólo un debate académico? La respuesta es lo que McAfee llama el marco Security Connected. Centralizando recursos tradicionalmente discrepantes entre varios proveedores, aprovechándolos para perfeccionarlos entre sí y alcanzando una alineación entre todas las contramedidas de seguridad, es posible reducir la complejidad, aumentar la eficacia operativa y disminuir los riesgos. Ello es semejante a un sistema de control de tráfico aéreo donde se agrega información extremamente complicada y discrepante y se hace manipulable a través de una "ventana" única.

Arquitectura de referencia Security Connected Nivel 2 – Temas por considerar

- Cómo proteger el Centro de datos
- Protección de dispositivos móviles

RESUMEN

Contemplar amenazas, tendencias y prioridades de negocios exige una estrategia de seguridad que proteja la actividad de su infraestructura de TI. Desde los ataques oportunistas y dirigidos hasta las tecnologías emergentes y el uso de la seguridad como una diferencia estratégica de negocios, el contar con una estrategia de seguridad conectada que no sólo llene los vacíos de la tecnología, sino que también considere las prioridades de negocios, puede afectar positivamente a la competitividad y al éxito de una empresa.

Muchas organizaciones probablemente se interesarán por algunos de esos temas (quizás todos ellos), pero hay otros igualmente importantes que no se abordaron. Si quiere conversar sobre esos y otros temas relacionados a la seguridad para comprender mejor nuestra posición y obtener más detalles sobre la Arquitectura de Referencia Security Connected de McAfee, visite www.mcafee.com/securityconnected.

El marco Security Connected de McAfee permite la integración de múltiples productos, servicios y alianzas para una disminución de riesgos centralizada, eficiente y eficaz. Con base en más de dos décadas de prácticas de seguridad probadas, el enfoque Security Connected ayuda a las organizaciones de todos los tamaños y segmentos, y en todas las regiones geográficas, a mejorar las posturas de seguridad, optimizarla para aumentar los ahorros, y a alinear estratégicamente la seguridad a las iniciativas de negocios. La Arquitectura de Referencia Security Connected proporciona una ruta concreta desde las ideas hasta su aplicación. Utilícela para adaptar los conceptos de Security Connected a sus riesgos, su infraestructura y sus objetivos de negocios específicos. En McAfee nos dedicamos incansablemente a encontrar nuevas formas de mantener la seguridad de nuestros clientes.

36502br_top-10-security_1211_wh

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com