Un mundo (de seguridad) nuevo:

Cambios que está experimentando la seguridad para dar cabida a la virtualización y la informática integrada en Internet

Un artículo técnico de Trend Micro™ | Enero de 2011

Escrito por Eva Chen

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

I. RESUMEN EJECUTIVO

En un futuro cercano, todo lo relacionado con las tecnologías de la información será móvil, dinámico e interactivo: acceso, datos, carga de trabajo y todos los aspectos informáticos. Los dispositivos móviles de los usuarios finales accederán y almacenarán cientos de gigabytes de datos. Los servidores virtuales distribuirán el rendimiento informático entre segmentos de red, centros de datos e incluso fuera del entorno corporativo, en la red pública, donde el rendimiento informático se ofrece como una prestación más.

Como resultado de estos profundos cambios, todos los aspectos relacionados con la seguridad informática se verán cuestionados y será necesario reconsiderarlos. La seguridad de redes tradicional, que abordaba fragmentos de capacidades informáticas como equipos y centros de almacenamiento de datos como si fueran un jardín vallado protegido, dejará de ser válida. Una nueva generación de prácticas de seguridad, que dan prioridad al dinamismo de la informática y los datos, pondrá en jaque el status quo establecido.

No obstante, este revolucionario cambio no se producirá de la noche a la mañana. El problema principal de las empresas será cómo afrontar el camino desde el punto en el que se encuentran hoy hasta al que se encontrarán en el futuro, pasando por un periodo de transición o híbrido. La solución a este reto no se reduce a un enfoque de "talla única" porque cada organización avanzará a su ritmo, en función de los requisitos a los que deba hacer frente y de otros muchos factores relacionados. Es por este motivo que las soluciones tienen que ofrecer la flexibilidad necesaria para albergar tanta diversidad. En este artículo técnico se aborda la evolución de los cambios que se están produciendo conforme las empresas empiezan a adoptar la virtualización y, posteriormente, la informática integrada en Internet. A continuación, se describe la visión de Trend Micro sobre la evolución de la seguridad como facilitador de la movilidad, la virtualización y la informática basada en Internet.

II. INTRODUCCIÓN

Según los analistas, el mercado de seguridad de redes mundial creció, en 2009, por encima de los 7.000 millones de $, mientras que el mercado de seguridad para puestos de trabajo/alojada creció más de 2.000 millones de $. ¿Por qué motivo es posible que la magnitud relativa de estos gastos oscile tanto en un futuro? La respuesta es que el mercado tradicional de la seguridad de redes se irá reduciendo conforme las redes vayan perdiendo relevancia a causa del dinamismo de las capacidades informáticas y los datos. En cambio, el mercado de la seguridad alojada, en el que la capacidad informática alojada y los datos están protegidos, crecerá exponencialmente: el alojamiento dinámico por si mismo tendrá que convertirse en el punto de protección principal.

El impacto que los cambios de esta evolución pueda tener en las tecnologías de la información y la seguridad es poco menos que espectacular. Supongamos que Bonnie y Clyde intentaran robar un banco hoy en día. Las artimañas a las que recurrían hace 100 años para robar bancos están totalmente obsoletas en la actualidad. Los bancos conservan cada vez menos dinero en efectivo disponible para los clientes, mientras que la banca electrónica cobra más importancia. Actualmente, la principal amenaza relacionada con los robos no consiste en atracar un banco a mano armada, sino en el robo de identidad, el robo de secretos empresariales olvidados en un iPad sin protección en un taxi y un amplio abanico de sofisticadas amenazas cibernéticas.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

La tendencia hacia la virtualización y la informática integrada en Internet es uno de los principales hilos conductores de este cambio de paradigma. Las empresas adoptan la virtualización y la informática en Internet ante las promesas de obtener numerosos beneficios para sus negocios, como flexibilidad de TI, escalabilidad, eficacia, reducción de costes y ventajas competitivas. Según un informe reciente de Gartner, "La virtualización continúa siendo el problema con mayor impacto al que deberán enfrentarse la infraestructura y las operaciones hasta el año 2015. Modifica la manera de gestionar, de comprar (cómo y qué se compra), de implementar, de planificar y de cobrar. También afecta significativamente a la obtención de licencias, a los precios y a la administración de componentes." [1] El alcance y la importancia de esta tendencia exige un análisis detallado del impacto y la función que debe tener la seguridad en la virtualización y la informática integrada en Internet.

III. REDES Y SEGURIDAD TRADICIONALES

Para entender mejor los retos y las oportunidades de seguridad que plantean la virtualización y la informática en Internet, resulta útil analizar primero la evolución de la seguridad desde las redes tradicionales antiguas hasta las redes actuales, así como la tendencia de esta evolución hacia la virtualización y la informática en Internet.

La Ilustración 1 muestra una red tradicional en la que tres de los principales tipos de recursos informáticos se encuentran dentro del perímetro de red: recursos informáticos en la DMZ, servidores básicos y puestos de trabajo. Esta disposición de seguridad relativamente sencilla consiste en cortafuegos, seguridad Web y de correo electrónico y sistemas de detección y prevención frente a intrusiones (IDS/IPS) en el perímetro de red. La seguridad basada en host consiste en implantar agentes antimalware en cada dispositivo informático que se halle dentro del perímetro.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

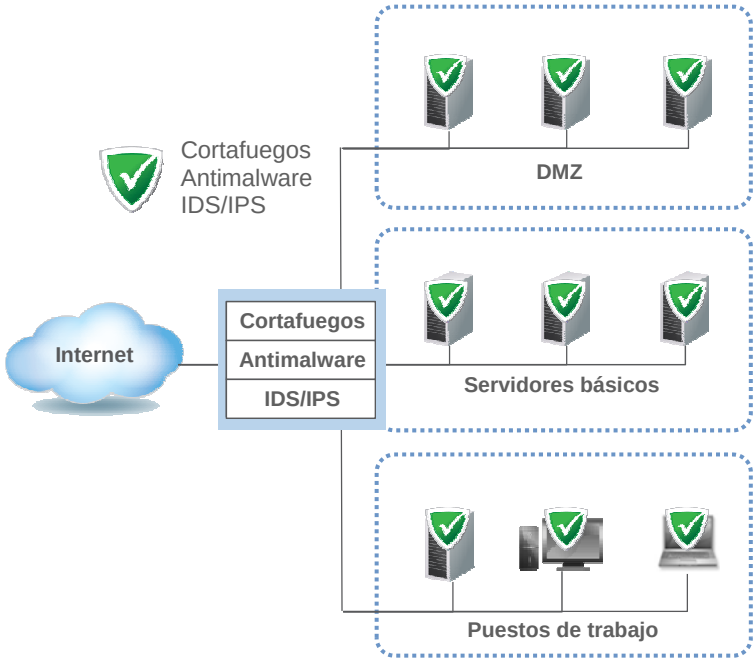

Ilustración 1. En una red tradicional, los agentes de seguridad basados en host de cada equipo incluyen principalmente antimalware, mientras que la seguridad del perímetro incluye un cortafuegos, seguridad Web y de correo electrónico e IDS/IPS.

A medida que los hackers descubrían el modo de acceder al perímetro de red a pesar de la seguridad existente y crecían las amenazas internas, los clientes se percataban de la necesidad de aumentar la protección en todos los dispositivos de la red (consulte la Ilustración 2). Para que los host se pudieran defender por sí mismos, los recursos de la DMZ, los servidores y los puestos de trabajo se equiparon con cortafuegos e IDS/IPS. Prácticamente en la misma época, surgieron nuevos dispositivos que ampliaron la definición de puesto de trabajo. Las empresas permitían que los empleados se conectaran a la red a través de los portátiles cada vez con más frecuencia. De ahí que las organizaciones tuvieran que ampliar sus redes para adaptarlas a estas herramientas. Dado que estos nuevos puestos de trabajo se desplazaban fuera de la red y se volvían a conectar, era necesario protegerlos con una seguridad aún más resistente. Asimismo, los agentes instalados en todos los dispositivos internos de la red (a los que se accedía de forma remota) requerían actualizaciones regulares por parte de algún tipo de red de protección y gestión centralizada.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

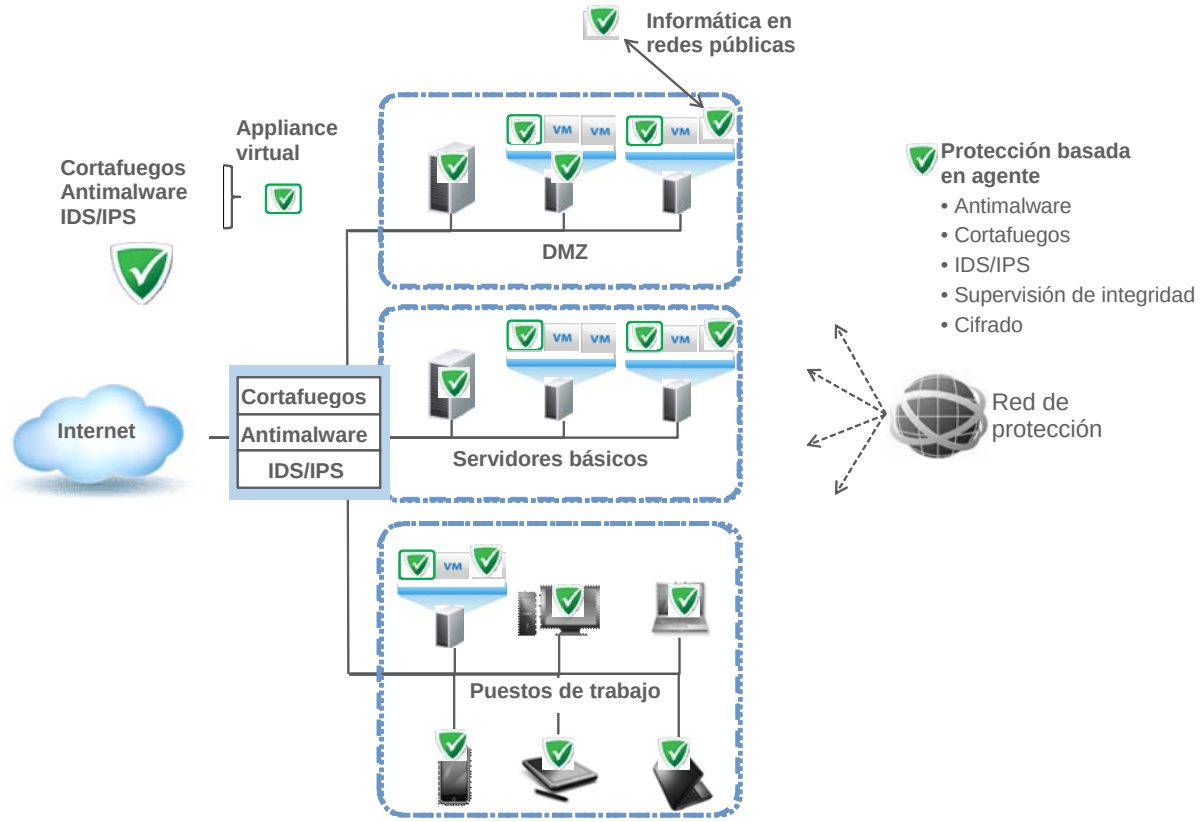

Ilustración 2. En muchas redes actuales, los agentes de host proporcionan una mayor protección, las redes se amplían para incluir puestos de trabajo móviles/remotos y se implementa algún tipo de red de protección.

IV. VIRTUALIZACIÓN

La virtualización resta relevancia al modelo de red tradicional, ya que la migración en vivo y la expansión dinamizan las aplicaciones y los datos, y los puntos conflictivos de la red se desvanecen. Ante esta "desperimetración", ahora resulta necesario ampliar la seguridad completamente a todos los nodos de host lógico, dondequiera que se encuentren los nodos.

Los agentes de seguridad de host proporcionan una seguridad más exhaustiva y pueden evolucionar paralelamente a las capacidades informáticas. Sin embargo, a medida que las empresas adoptan la virtualización, la implementación de un agente de seguridad de host en cada uno de los host se hace más difícil y mantener la naturaleza "instantánea" de estos servidores y equipos de sobremesa virtuales se convierte en un gran problema.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

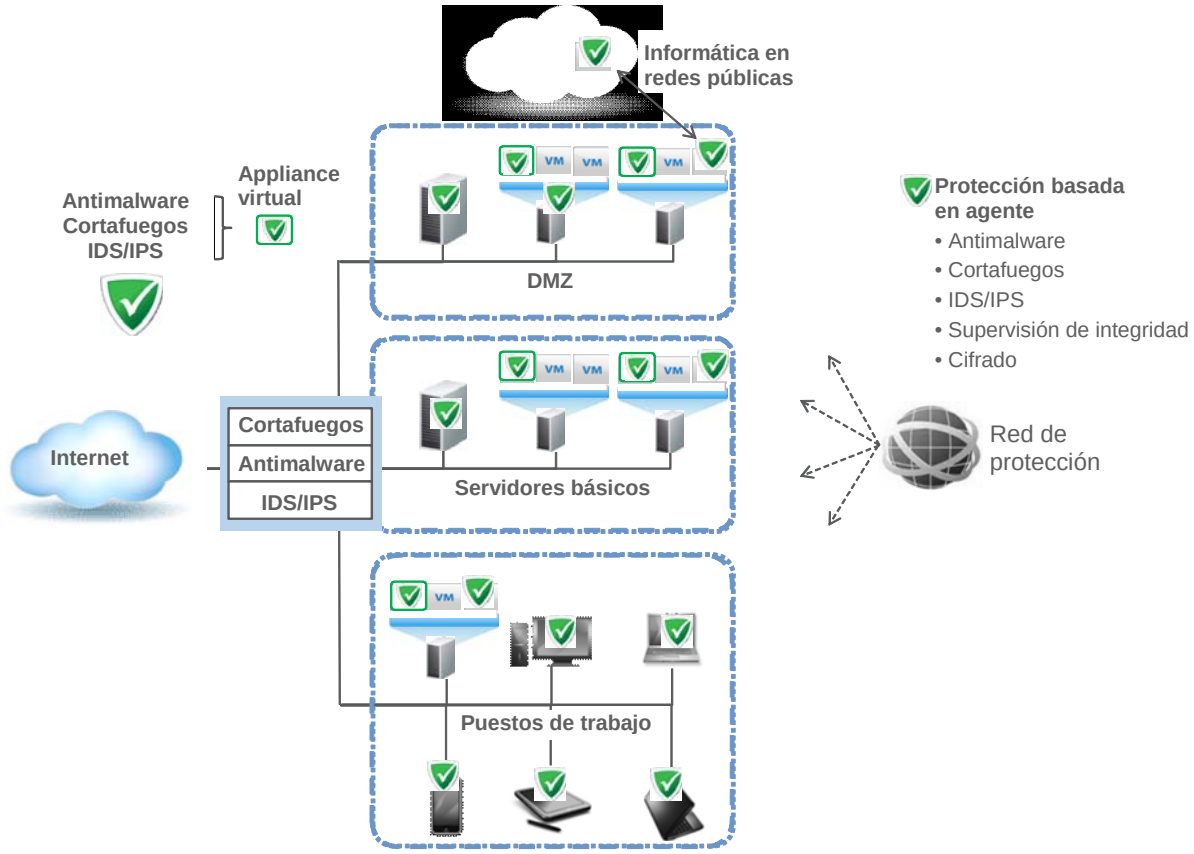

Ilustración 3. Cuando las organizaciones evolucionan hacia la virtualización, el modelo de red tradicional pierde relevancia y es necesario ampliar la seguridad a todos los nodos de host lógico. En la ilustración, observamos el modo en que un appliance virtual amplía la seguridad a los equipos virtuales.

A medida que empiezan a implementar la virtualización, las organizaciones suelen añadir equipos virtuales (EV), inicialmente en los equipos físicos tradicionales mediante disposiciones híbridas, tal y como se muestra en la Ilustración 3. Para proporcionar la seguridad necesaria, las empresas necesitan un appliance virtual (una imagen de software diseñada para ser ejecutada en un equipo virtual). La introducción de este appliance permite a las organizaciones mejorar la seguridad en el hipervisor para garantizar una protección más eficaz. De este modo también consiguen aportar visibilidad al tráfico entre EV y disfrutar de otras ventajas de seguridad específicas de la virtualización, como la seguridad entre EV, los parches virtuales para los host que se crean y la eficacia del rendimiento del módulo antimalware.

El appliance virtual se implementa para proteger cada uno de los EV que controla. Ahora, cada equipo físico funciona casi como una red. Dado que las organizaciones tienden a utilizar aplicaciones similares en los mismos equipos físicos, la implementación de un appliance virtual les permite configurar reglas de seguridad más detalladas en dicho extremo virtual, en comparación con las reglas de seguridad del perímetro del centro de datos, de cariz más general. Este enfoque también simplifica el funcionamiento de la edición de reglas para el cortafuegos o IDS/IPS del perímetro. Del

mismo modo, esta disposición proporciona una protección "sin agente" para el segmento completo de la red virtual. Con ello, se mejora el rendimiento de la estructura general y se garantiza la seguridad básica en caso de que el agente de seguridad del host todavía no se haya implementado o no exista debido a una limitación de la plataforma. El appliance de seguridad virtual también puede proporcionar la función de control de admisión a la red (NAC) y puede informar o alertar a un administrador, o bien evitar que un EV con una seguridad inadecuada se inicie en un servidor o se traslade al mismo.

Por este motivo, mientras se consolida el centro de datos, el nuevo modelo de seguridad pone de manifiesto la importancia de una defensa exhaustiva, donde:

1. La seguridad del perímetro, como los cortafuegos o IDS/IPS tradicionales, continúa en primera línea, sobre todo en la defensa contra ataques del exterior, es decir, los intentos de traspasar la primera línea de defensa desde fuera.

2. Los appliances virtuales del extremo de la red virtual funcionan con reglas de seguridad más granulares, relacionadas especialmente con la seguridad de las aplicaciones y la protección virtual. Este hecho no solo mejora la seguridad del perímetro, sino que también reduce la frecuencia de los cambios que se deben realizar en los dispositivos del perímetro. Asimismo, esta capa también proporciona la seguridad básica necesaria en caso de que no se implemente ningún agente de seguridad del host.

3. La inclusión de un agente de seguridad basado en host en cada uno de los host permite detectar y modificar dinámicamente la política de seguridad a medida que la informática/carga de trabajo se trasladan, por ejemplo, del interior de la red corporativa al modo roaming del exterior, a otro centro de datos o a Internet.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

Este enfoque introduce el concepto de seguridad "sintonizada a las necesidades". La seguridad "bien sintonizada" para mejorar la protección consume recursos del sistema y del personal de TI, pero la seguridad "mal sintonizada" reduce la protección a la vez que conserva los recursos del sistema y del personal de TI. Las consideraciones que influyen en el nivel de seguridad necesario incluyen los requisitos de las normativas, la naturaleza de sensibilidad/confidencialidad de los datos y las políticas de seguridad. Es más sencillo encontrar el equilibro adecuado de forma individualizada, ya que la protección se implementa más cerca del destino objetivo del tráfico entrante. El motivo es que la seguridad del perímetro debe explorar todo el tráfico entrante de la red, lo cual resulta una tarea complicada debido a los diferentes tipos de tráfico existentes (como el basado en Linux, UNIX y Microsoft Windows) vinculados a distintas partes de la red con propósitos diferentes. No obstante, explorar más cerca del objetivo puede resultar más granular, ya que solo determinados tipos de tráfico son adecuados para el objetivo, como el tráfico de Linux para tráfico vinculado a dicha plataforma. Es por ello que la exploración de appliances virtuales puede resultar más eficaz: el appliance virtual está más cerca del destino objetivo de lo que estaría un dispositivo de exploración del perímetro.

Transformación radical en los puestos de trabajo

La virtualización conlleva una transformación radical de los puestos de trabajo. Antes de la virtualización, la actividad de un usuario estaba vinculada a un único equipo de sobremesa físico o al nodo de un equipo portátil, protegido por un agente instalado. Hoy en día, la virtualización de los equipos de sobremesa, que ejecuta los equipos de sobremesa en el centro de datos, es una realidad. Sin embargo, los cambios en los equipos de sobremesa son de mayor envergadura que la transferencia del sistema operativo (SO) y las aplicaciones a un EV del centro de datos. El equipo de sobremesa se descompone en la prevención y detección de intrusiones de servidor con SO, las aplicaciones y los usuarios reales que se gestionan y almacenan de forma diferenciada para recomponerse a través de la red en un espacio de trabajo aparentemente familiar para cada usuario tras el inicio de sesión. El SO se descompone además en imágenes maestras comunes para el resto de usuarios y "variaciones" específicas de cada usuario. Las aplicaciones parecen locales, pero pueden transmitirse al espacio de trabajo mientras en realidad se ejecutan en otro EV o como una aplicación de software como servicio (SaaS) en la red pública.

En la actualidad, es un cliente físico el que accede a este espacio de trabajo de forma cada vez más remota y móvil. La tendencia de los terminales delgados se está extendiendo a los iPads y otras tabletas, a los teléfonos multifunción y a los equipos informáticos "hechos en casa". La posibilidad de acceder al equipo de sobremesa virtual desde varias ubicaciones y dispositivos ha ampliado el espacio de trabajo del usuario, que ahora es prácticamente ilimitado. El equipo de sobremesa ha pasado a ser móvil, ubicuo, delgado y heterogéneo.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

V. INFORMÁTICA INTEGRADA EN INTERNET

La virtualización es un catalizador de la informática basada en Internet. Por ejemplo, acelera la transformación de los centros de datos en redes privadas. A medida que las organizaciones evolucionan hacia la informática en Internet, les es posible trasladar aplicaciones de sus recursos a los recursos de Internet, y a la inversa, para obtener beneficios empresariales.

No obstante, beneficiarse de esta eficiencia informática aumenta la presión del modelo de seguridad. Como se ha mencionado anteriormente, los agentes son necesarios para el traslado de la carga de trabajo, que incluye el sistema operativo, las aplicaciones y los datos. Sin embargo, los requisitos empresariales como el estricto cumplimiento de las normativas requieren agentes "avanzados" más sofisticados que puedan ajustar el nivel de protección para adaptarlo a varias tareas. Las empresas están sometidas a mucha presión para cumplir una gran variedad de normativas y estándares como el Estándar de seguridad de datos de la industria de pagos con tarjeta (PCI DSS), la Ley estadounidense de portabilidad y responsabilidad del seguro médico (HIPAA) y la Ley estadounidense Gramm-Leach-Bliley (GLBA), así como prácticas de auditoría como la Declaración de estándares de auditoría (SAS70) y los estándares de la Organización internacional para la estandarización (ISO). Asimismo, deben demostrar el cumplimiento de los estándares de seguridad, independientemente de la ubicación de los sistemas regulados, incluidos los servidores in situ, los equipos virtuales in situ y los equipos virtuales situados fuera de las instalaciones que se ejecutan en recursos basados en Internet.

Ante esta situación, el antimalware, los cortafuegos y el sistema IDS/IPS no son suficientes para la protección basada en agentes (consulte la Ilustración 3). Algunas de las normativas indicadas anteriormente incluyen requisitos de cifrado para proteger la información fundamental, como los datos de los titulares de tarjetas e información de identificación personal. Estos requisitos pueden incluir el cifrado de disco completo (FDE), la seguridad del Estándar de cifrado avanzado (AES) y la seguridad normativa de los Estándares de procesamiento de información federal (FIPS) 140-2. La naturaleza multiempresa de Internet amplifica estos requisitos. Es necesario supervisar la integridad del sistema operativo y los archivos de aplicaciones críticos para detectar cambios maliciosos o inesperados que podrían indicar riesgos en los recursos informáticos. Asimismo, se deben inspeccionar los registros para proporcionar visibilidad de los eventos de seguridad importantes escondidos en los archivos de registros de los recursos de Internet. La Ilustración 1 muestra que los controles de seguridad utilizados en el enfoque tradicional también son necesarios en un entorno de Internet híbrido nuevo.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

Control de seguridad	Red tradicional (jardín vallado)		Red nueva (entorno de Internet híbrido)
Cortafuegos	✓		✓
IDS/IPS	✓		✓
Protección de aplicaciones Web	✓		✓
Supervisión de la integridad de los archivos	✓		✓
Inspección de registros	✓		✓
Antimalware	✓		✓
Cifrado	✓		✓
Mensajería	✓		✓

Ilustración 1. Los controles de seguridad utilizados en el enfoque tradicional también son necesarios en un entorno de Internet híbrido nuevo.

VI. VISIÓN DE TREND MICRO

Con el objetivo de proporcionar una seguridad eficaz en la era de la virtualización y la informática en Internet, la seguridad de última generación debe incluir una combinación óptima de enfoques que proteja los recursos físicos tradicionales, los recursos virtuales y las cargas de trabajo dondequiera que estén ubicadas, incluido el entorno de Internet (consulte la Ilustración 4). Trend Micro Smart Protection Network™ proporciona supervisión y se asegura de que la protección de todos los recursos y los agentes de carga de trabajo sea resistente y se mantenga actualizada. La seguridad se traslada con las cargas de trabajo según las necesidades específicas y se implementa en el hipervisor para proteger todos los sistemas operativos invitados desde una única ubicación.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

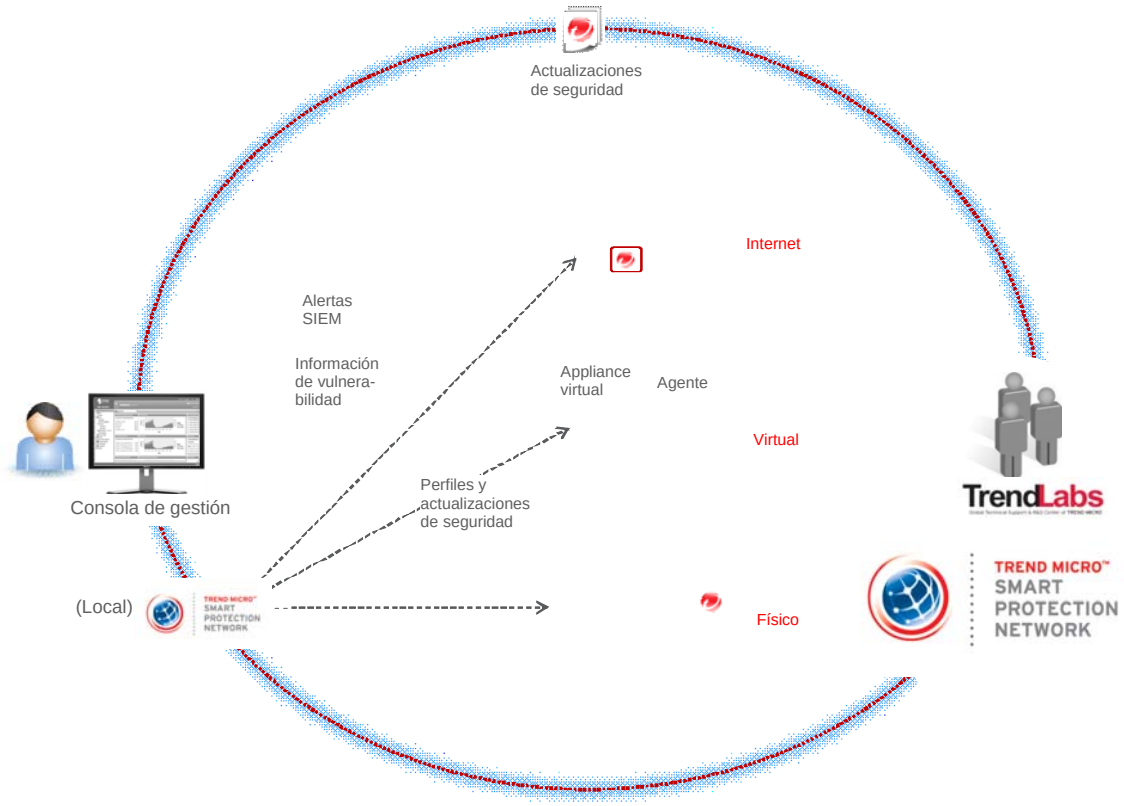

Ilustración 4. La visión de Trend Micro de la seguridad de última generación incluye una combinación óptima de enfoques que protege los recursos físicos tradicionales, los recursos virtuales y las cargas de trabajo dondequiera que estén ubicadas, incluido el entorno de Internet.

El host proporcionará la mayor parte de la funcionalidad de seguridad necesaria en un entorno virtualizado y, en última instancia, de Internet. Estos controles de seguridad basados en host representarán la virtualización de la seguridad, lo cual significa, en primer lugar, que la seguridad deberá mantener el servicio instantáneo, que es el distintivo de la virtualización. Sin embargo, esto puede convertirse en una oportunidad, ya que es posible implementar inmediatamente una política de seguridad definida cada vez que se proporciona servicio a un nuevo dispositivo. Esto es un ejemplo del modo en que la virtualización ofrece una enorme y emocionante oportunidad para aumentar la seguridad. Esta evolución de la seguridad también proporciona oportunidades para evitar los periodos de inactividad que se producen como resultado de una infección o una infracción de seguridad, lo cual permite mantener la continuidad del negocio y ayuda a garantizar el cumplimiento de las normativas.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

En este paradigma dominado por el host, es probable que los proveedores de servicios de seguridad que tienen experiencia en el diseño y la implementación de seguridad basada en host estén en una posición más favorable para ofrecer esta seguridad virtualizada ampliada y mejorada a las organizaciones. Diseñar la seguridad de un gran número de host y puestos de trabajos es totalmente diferente a diseñar la seguridad de una red. Los proveedores experimentados que abordan las necesidades y oportunidades específicas de la seguridad basada en host, así como los que desarrollan las prácticas recomendadas en este espacio, tienen más posibilidades de liderar la próxima generación de servicios de seguridad.

Este cambio modificará el modo de invertir el dinero de TI en seguridad, y las soluciones basadas en host recibirán gradualmente más atención y presupuesto. No obstante, el cambio no se producirá de la noche a la mañana. La migración de los cortafuegos a los equipos de sobremesa tardó aproximadamente diez años en realizarse; por su parte, la evolución de las redes tradicionales a la virtualización en primer lugar y, más tarde, a la informática en Internet también llevará su tiempo.

VII. CARACTERÍSTICAS DE LA ESTRATEGIA DE SEGURIDAD DE ÚLTIMA GENERACIÓN

Trend Micro trabaja con la premisa de una estrategia de seguridad de próxima generación: una estrategia con la que las empresas realmente podrán materializar las importantes ventajas empresariales y la reducción de costes generadas por la virtualización y la informática integrada en Internet. Todo ello, gracias a los siguientes elementos que ya se comercializan en la actualidad:

- **Arquitectura basada en Internet:** la seguridad debería construirse desde los cimientos a fin de poder integrarla con las tecnologías y los modelos de virtualización e informática basada en Internet y aprovechar así sus ventajas.
- **Movilidad:** en un mundo dominado por una movilidad en aumento, gracias a las redes 3G, vMotion, la informática integrada en Internet y la consumerización de dispositivos de TI como los teléfonos multifunción y las tabletas, la seguridad también tiene que ser móvil. Debe viajar con los datos, las aplicaciones y los dispositivos cuya protección se le ha encomendado.
- **Puestos de trabajo ligeros:** la presencia de la protección en los puestos de trabajo debe reducirse a la mínima expresión posible a fin de ser viable en los dispositivos más pequeños y/o delgados tales como equipos virtuales, teléfonos multifunción y dispositivos basados en USB. Además, debe consumir los mínimos recursos de memoria, tiempo de CPU y E/S.
- **Velocidad:** la seguridad debe ser ágil de aplicar, rápida de actualizar (dado el ritmo de detección de nuevas amenazas y vulnerabilidades y la velocidad a la que los equipos virtuales pueden gestionarse o modificarse de un estado en espera a uno en activo) y causar un impacto mínimo en el rendimiento del sistema.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

- **Sencillez:** la seguridad debería ser fácil de utilizar y fácil de integrarse con las soluciones y la infraestructura de TI existentes, además de incluir funciones de automatización, notificación, generación de informes y otras características que reducen el tiempo de gestión y mantenimiento.

- **Cobertura de la protección:** debería virtualizarse una amplia gama de controles de seguridad básicos (entre los que se incluyen antivirus, cifrado, prevención de la pérdida de datos (DLP), cortafuegos, IDS/IPS, supervisión de integridad de archivos e inspección de registros), que además deberían integrarse a la perfección en entornos virtualizados y de informática integrada en Internet. Las soluciones de seguridad específicas no son suficientes.

- **Protección eficaz, accesible, compatible y acorde a la normativa:** ante el auge de la consumerización y de los modelos de suministro de equipos personalizados, las soluciones de seguridad deberían estar disponibles globalmente y accesibles fácilmente para los consumidores, ofrecer una protección eficaz, funcionar de acuerdo con los estándares informáticos corporativos y, por último, contar con un respaldo global.

- **Políticas y controles:** en un futuro no muy lejano, serán muchas las empresas que tengan que compatibilizar un modelo híbrido de recursos físicos, virtuales y de servicios en la red. Ante este cambio de tendencia, las políticas y los controles de seguridad deberán estar disponibles de manera sistemática y estar presentes en estos tres entornos diferenciados.

VIII. SOLUCIONES DE TREND MICRO

Las soluciones avanzadas diseñadas específicamente para proteger este entorno pueden disminuir el riesgo, mejorar el rendimiento, simplificar la gestión y, en última instancia, garantizar la seguridad de los centros de datos en el futuro. En este escenario, Trend Micro ofrece una seguridad diseñada para los entornos virtualizados y basados en Internet. Trend Micro lidera la innovación en protección de datos, tecnologías diseñadas para el futuro como Trend Micro Smart Protection Network™ y en soluciones que garantizan la continuidad empresarial y el cumplimiento de las normativas. Trend Micro ofrece las soluciones siguientes en este campo:

- Trend Micro™ Deep Security ofrece protección avanzada para los sistemas de centros de datos dinámicos, ya sean equipos de sobremesa físicos o servidores virtuales o basados en Internet. Deep Security combina funciones de detección y prevención de intrusiones, cortafuegos, supervisión de la integridad, inspección de registros y antimalware en una única solución de software empresarial de gestión centralizada. La solución puede implementarse con dos configuraciones: sin agente (appliance virtual) o con agente.

- Trend Micro™ SecureCloud™ es una solución alojada para la gestión de claves y el cifrado de datos diseñada para proteger y controlar la información confidencial que se implementa en entornos informáticos integrados en Internet públicos y privados. SecureCloud es eficaz y fácil de usar, ayuda a garantizar el cumplimiento de las normativas y permite elegir libremente proveedores de servicios en la red al no exigir vinculación con ningún sistema de cifrado de un proveedor.

UN MUNDO (DE SEGURIDAD) NUEVO: CAMBIOS QUE ESTÁ EXPERIMENTANDO LA SEGURIDAD PARA DAR CABIDA A LA VIRTUALIZACIÓN Y LA INFORMÁTICA INTEGRADA EN INTERNET

- Trend Micro™ OfficeScan™ brinda protección para los equipos de sobremesa virtuales y físicos, conectados o no a la red corporativa. Se trata de la primera solución de infraestructura de equipos de sobremesa virtuales (VDI) del sector optimizada para la seguridad de los puestos de trabajo. Agiliza la protección, reduce el consumo de recursos y permite la aplicación virtual de parches.

- La infraestructura Trend Micro™ Smart Protection Network™ permite una protección avanzada en Internet gracias al bloqueo de las amenazas en tiempo real, antes de que lleguen a los usuarios. Basada en una exclusiva arquitectura informática integrada en Internet, cuenta con una red mundial de sensores de información sobre las amenazas y tecnologías de reputación de correo electrónico, Internet y archivos que trabajan conjuntamente para reducir drásticamente las infecciones.

- Trend Micro™ Mobile Security protege los teléfonos multifunción y PDA frente a la pérdida de datos, infecciones y ataques desde una consola empresarial centralizada que también permite gestionar la protección de los equipos de sobremesa.

Trend Micro brinda productos de seguridad probados, fiables y listos para su uso, según certifican las autoridades competentes. Si desea más obtener más información, visite www.trendmicro.com/virtualization.

IX. PRÓXIMOS PASOS

Las empresas que buscan ayuda para implementar sus iniciativas de virtualización e informática integrada en Internet deberían plantear las siguientes preguntas clave a sus proveedores:

- ¿Cómo y cuándo aplicó el proveedor las últimas API de seguridad en virtualización de VMware y otros proveedores líderes del mercado?

- ¿Cuál es la hoja de ruta del proveedor en cuanto a productos de seguridad móvil para el consumidor? ¿Cuentan con alguna solución para proteger tabletas, teléfonos multifunción y otros dispositivos móviles?

- ¿Qué arquitectura Internet-cliente utiliza el proveedor? ¿Hasta qué punto aprovechan la informática integrada en Internet para mejorar la eficacia de la protección?

La transición a la virtualización y, posteriormente, a la informática integrada en Internet tendrá como consecuencia disposiciones informáticas híbridas que pueden presentar vulnerabilidades y problemas de seguridad. La duración de este periodo de transición, entre moderado y largo, implica para muchas empresas tener que colaborar estrechamente con un partner de seguridad que les ayude a garantizar una seguridad eficaz durante todas las fases de la transición. Este proveedor debería ofrecer un exhaustivo registro de seguimiento de la seguridad basada en host (porque la seguridad de la virtualización y la informática basada en Internet reside principalmente en el host) y disponer de una visión de futuro bien analizada.

X. CONCLUSIÓN

El mundo de TI evoluciona rápidamente y tanto consumidores como empleados adoptan los dispositivos móviles que se comercializan casi de la noche al día. La movilidad es la reina. Las empresas pretenden obtener beneficios de la virtualización y la informática basada en Internet cuanto antes mejor. Como elemento facilitador de estos cambios, y para que las empresas se percaten de las ventajas existentes, la seguridad puede hacer el camino más fácil durante los difíciles periodos de transición que se avecinan. Para lograrlo, el sitio de la seguridad está cambiando de la red al host. Trend Micro, como proveedor líder de soluciones tecnológicas basadas en host desde hace 22 años, se encuentra en una posición única para guiar a los líderes del sector durante los tiempos de cambios.

XI. SI DESEA OBTENER MÁS INFORMACIÓN

Si desea más obtener más información, visite www.trendmicro.com/virtualization.

XII. ACERCA DE TREND MICRO

Trend Micro Incorporated, líder mundial en la seguridad de contenidos en Internet y gestión de amenazas, tiene como objetivo crear una caja fuerte mundial para el intercambio de información digital entre empresas y consumidores. Trend Micro, empresa pionera en soluciones antivirus basadas en servidores y con más de 20 años de experiencia, ofrece seguridad del más alto nivel adaptada a las necesidades de nuestros clientes, detiene las amenazas más rápidamente y protege la información en entornos físicos, virtualizados y basados en Internet. Con el respaldo de la infraestructura de Trend Micro™ Smart Protection Network™, nuestra tecnología y nuestros productos de seguridad basados en Internet líderes del sector consiguen detener las amenazas allá donde surgen, en Internet, y cuentan con la asistencia de un equipo de más 1.000 expertos en amenazas en todo el mundo. Si desea más obtener más información, visite www.trendmicro.com.

Más información en www.trendmicro.com.

XIII. REFERENCIA

1. “ATV: Virtualization Reality,” Informe de investigación Gartner. Número de ID G00205779, 30 de julio de 2010.