

Seguridad de la informática en Internet

Seguridad del servidor



Preparación de
equipos virtuales
para Internet

Artículo técnico
de Trend Micro | Agosto de 2009

I. INTRODUCCIÓN

La informática en Internet (*Cloud computing*) se ha comparado a la temprana propagación de la electricidad: ni las casas, ni los negocios ni las ciudades quisieron producir o basarse en una fuente de energía propia, sino que comenzaron por conectarse a una rejilla de potencia mucho mayor que se mantenía y controlaba a través de servicios de energía. Esta conexión mediante servicios reportó un ahorro de tiempo y de dinero, unido a un mejor acceso a la energía que, además, estaba disponible de forma más fiable.

De un modo parecido, la informática en Internet constituye una oportunidad de enorme peso para los proveedores de servicio y las empresas. Así, gracias a la informática en Internet, las empresas logran ahorros económicos, flexibilidad y una gama de recursos informáticos, por lo que recurren a ella para ampliar sus infraestructuras in situ al poder añadir más capacidad según la demanda.

Este documento trata de la variación de la informática en Internet, también conocida como informática de servicio o infraestructura como servicio (IaaS). Se centra en las implicaciones de seguridad y los retos que la IaaS plantea y, asimismo, provee a las empresas y a los proveedores de servicio de mejores prácticas para ayudar a sacar partido de IaaS con el fin de mejorar los resultados empresariales en el clima económico extremo de hoy día.

II. LA OPORTUNIDAD DE LA INFORMÁTICA EN INTERNET

Ampliar las fronteras fuera de la organización para aumentar la competitividad no es ninguna novedad; es, sencillamente, un proceso de externalización. Entonces, ¿qué lleva a tanto alboroto y excitación con la informática en Internet?

Impulso del sector: diversos analistas del sector y compañías como, entre otras muchas, Amazon, Citrix, Dell, Google, HP, IBM, Microsoft, Sun o VMware, han manifestado su apoyo unánime a la informática en Internet. En septiembre de 2008, la iniciativa vCloud de VMware supuso el primer ejemplo de un proveedor de tecnología que condensaba a proveedores de servicios, aplicaciones y tecnologías para aumentar la disponibilidad y las oportunidades de las empresas a la hora de beneficiarse de la informática en Internet.

Flexibilidad: la flexibilidad en las empresas es inaudita. Así, las empresas pueden optar por externalizar el hardware pero conservar el control de la estructura de TI; externalizar totalmente todos los aspectos de la infraestructura, o (motivadas a menudo por iniciativas de departamentos) implementar en sus infraestructuras segmentos externalizados tanto parcial como completamente.

Terminología de la informática en Internet

IaaS: *infraestructura como servicio, también denominada "informática de servicio", "servicio de infraestructura" o "informática de instancias**", donde la infraestructura física se compone de instancias virtuales de los recursos necesarios. Ejemplos de proveedores: Amazon EC2, GoGrid*

PaaS: *plataforma como servicio, también descrita por el analista de Redmonk Stephen O'Grady* como "informática de tejido*", donde la arquitectura lógica y física subyacente se abstrae. Ejemplos: Google App Engine, Microsoft Azure*

SaaS: *software como servicio, que hace referencia al acceso basado en Internet a determinadas aplicaciones. Ejemplo: Salesforce.com, Workstream*

**<http://redmonk.com/sogradey/topic/cloud>*

SEGURIDAD DE LA INFORMÁTICA EN INTERNET

PREPARACIÓN DE EQUIPOS VIRTUALES PARA INTERNET

Ahorro de costes: la infraestructura a petición deriva en un gasto de TI más eficaz. Con bastante frecuencia, las limitaciones en el número de empleados y las inversiones de capital frenan la posibilidad de innovación. Las demandas temporales anulan los requisitos de capacidad y obligan a una infraestructura sólida que, muchas veces, no se utiliza. La informática en Internet es una alternativa rentable a esto.

Movilidad y elección: la tecnología lidera la evolución. Las distintas tecnologías de virtualización, como Vmware, permiten que las aplicaciones y servicios pasen de los entornos internos a las redes públicas o de un proveedor de servicios de Internet a otro.

ESCALABILIDAD:

La infraestructura como servicio (IaaS) es sinónimo de escalabilidad. ¿Necesita disponer de servidores imperiosamente, pero no hay tiempo para lograr adquisiciones de capital? Solo hace falta una tarjeta de crédito para hacerse con la infraestructura que desee. Los departamentos y las pequeñas empresas (incluidos los proveedores de servicios o de servicios gestionados de menor tamaño) que necesitan capacidad a petición están preparados para aprovechar las ventajas de la informática en Internet. La conmutación por error y la redundancia son también aspectos de gran impacto que llevan a recurrir a la informática en Internet.

En esencia, la informática en Internet amplía la capacidad de una empresa de cubrir la demanda informática en sus operaciones cotidianas. En tanto ofrece flexibilidad, posibilidad de elección, movilidad y escalabilidad (aparte de un más que probable ahorro de costes), la ventaja que reporta la informática en Internet es reseñable. Sin embargo, existe un aspecto que hace que las organizaciones sean reticentes a la hora de trasladar las cargas de trabajo de sus negocios a las redes públicas: la seguridad.

En este sentido, IDC realizó una encuesta entre 244 directores/ ejecutivos de TI y sus colegas de línea de negocios para evaluar sus opiniones y saber el uso que sus compañías hacían de los servicios informáticos de Internet. La seguridad obtuvo el primer puesto como principal desafío o problema achacable a la informática en Internet.

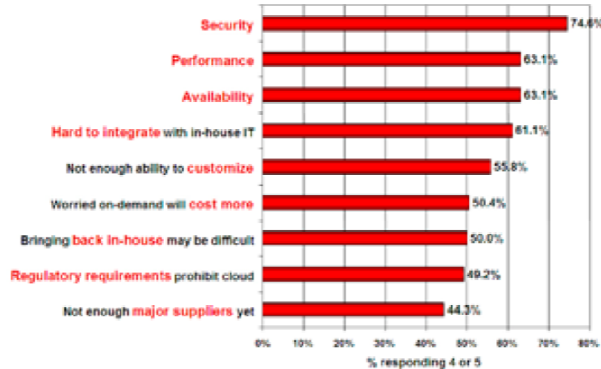
¿Cómo se aterriza en la informática en Internet?

Las empresas acaban por usar la informática en Internet de dos maneras. Por un lado, los directores, ante la evidente tentación de aspectos como una mayor ventaja competitiva, el ahorro de costes, una capacidad ampliada y la flexibilidad de conmutación por error, sopesan la posibilidad de la informática en Internet y se plantean cómo mantener la política de seguridad y la integridad del cumplimiento en este entorno nuevo y dinámico. Por otro, los departamentos o grupos de trabajo, ansiosos por disponer de recursos y resultados informáticos inmediatos, se están subiendo al carro de la informática en Internet, probablemente sin tener en cuenta ninguna de las implicaciones de seguridad necesarias a la hora de colocar los datos y aplicaciones críticos en un entorno de Internet.

SEGURIDAD DE LA INFORMÁTICA EN INTERNET

PREPARACIÓN DE EQUIPOS VIRTUALES PARA INTERNET

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

“La seguridad es, con mucho, el principal problema de los servicios por Internet. Al ver la información y recursos de TI fundamentales de sus negocios fuera de la protección del cortafuegos, los clientes se preocupan ante la posibilidad de sufrir un ataque.”

– Frank Gens, vicepresidente y analista jefe, IDC

III. SEGURIDAD Y CUMPLIMIENTO EN LA INFORMÁTICA EN INTERNET

El hecho de sacar los equipos virtuales, con todas las aplicaciones críticas y los datos confidenciales, de las instalaciones a entornos informáticos compartidos y de carácter público plantea una serie de retos de seguridad a las organizaciones que, hasta ahora, se habían basado en la defensa perimetral de la red como método principal de protección del centro de datos. Esto también puede conllevar una anulación del cumplimiento y una infracción de las políticas de seguridad. Los directores, ante la evidente tentación de aspectos como una mayor ventaja competitiva, el ahorro de costes, una capacidad ampliada y la flexibilidad de conmutación por error, sopesan la posibilidad de la informática en Internet y se hacen las siguientes preguntas:

- ¿Seguiré teniendo el mismo control de políticas de seguridad sobre las aplicaciones y servicios?
- ¿Puedo demostrar a mi organización y clientes que sigo disfrutando de la misma seguridad y cumpliendo los acuerdos de nivel de servicio?
- ¿Sigo dentro de la normativa y puedo demostrarlo a mis auditores?

Para empezar a responderlas, echemos un vistazo rápido a la seguridad de un centro de datos tradicional y el impacto de la tecnología de virtualización, que está dando pie a la revolución de la informática en Internet.

SEGURIDAD DE UN CENTRO DE DATOS TRADICIONAL

El concepto de 'centro de datos' siempre ha despertado imágenes de conjuntos de servidores mastodónticos ocultos tras puertas infranqueables, donde la electricidad y el enfriamiento eran igual de importantes que la seguridad de la red para mantener la fiabilidad y la disponibilidad de los datos. Los controles de seguridad perimetral constituyen el principal método adoptado en la seguridad de un centro de datos tradicional. Este método suele incluir un cortafuego perimetral, zonas desmilitarizadas, segmentación de la red, sistemas de detección y prevención de intrusiones y herramientas de supervisión de la red.

VIRTUALIZACIÓN: EL CATALIZADOR DE INTERNET

Los avances en tecnología de virtualización permiten que las empresas logren una mayor potencia de los equipos a partir de la capacidad infrautilizada de los servidores físicos. El impacto de los centros de datos tradicionales se está reduciendo para dar paso a un ahorro de costes y una TI "más verde" gracias a la consolidación de servidores. Las empresas y los proveedores de servicios usan la virtualización para dar pie a un uso multiempresarial de lo que antes eran servidores físicos de empresa u objetivo únicos.

La extensión de los equipos virtuales a las redes públicas hace que el perímetro de la red empresarial se evapore y que hasta el más mínimo denominador común tenga impacto en la seguridad global. La incapacidad de la seguridad basada en el hardware y la segregación física de hacer frente a los ataques entre los equipos virtuales en el mismo servidor acucia la necesidad de disponer de mecanismos que se implementen directamente en el servidor o en los equipos virtuales.

Si esta línea de defensa se implementa en el propio equipo virtual, las aplicaciones y datos críticos podrán trasladarse a entornos basados en Internet.

"En un entorno de TI en el que cada vez son más los recursos informáticos y de almacenamiento que se agregan en menos dispositivos físicos y centros de datos, resulta difícil dar con una estrategia que distribuya los recursos en zonas con dispositivos en línea para filtrar el tráfico y controlar el acceso a dichas zonas. Esto, además, puede reducir la economía de escala y otras ventajas operativas de la consolidación en la infraestructura de TI."

Burton Group, "Network Security in the Real World", Phil Schacter, Eric Maiwald, octubre de 2008

IV. DESAFÍOS DE LA SEGURIDAD EN INTERNET

A simple vista, puede parecer que los requisitos de seguridad de los proveedores de informática en Internet son los mismos que los de los centros de datos tradicionales: crear un perímetro de seguridad de la red sólido e impedir que los chicos malos se abran paso. Sin embargo, tal y como se ha descrito anteriormente, la seguridad basada en el hardware y la segregación física no sirve de protección frente a los ataques entre los equipos virtuales en el mismo servidor. Para que los proveedores de informática en Internet disfruten de la eficacia de la virtualización, los equipos virtuales de varias organizaciones deberán residir conjuntamente en los mismos recursos físicos. A continuación se explican algunos de los principales problemas que toda empresa debería tener en cuenta a la hora de planificar sus implementaciones de informática en Internet.

ACCESO ADMINISTRATIVO A SERVIDORES Y APLICACIONES

Una de las características primordiales de la informática en Internet es que proporciona acceso de "autoservicio" a la potencia de los equipos, sobre todo a través de Internet. En los centros de datos tradicionales, el acceso administrativo a los servidores se controla y limita a las conexiones directas o in situ, mientras que con la informática en Internet este acceso se puede realizar a través de Internet, lo cual supone un aumento del riesgo y la exposición. En consecuencia, es muy importante restringir el acceso administrativo y supervisarlos para mantener la visibilidad de los cambios en el control del sistema.

EQUIPOS VIRTUALES DINÁMICOS: ESTADO Y EXPANSIÓN

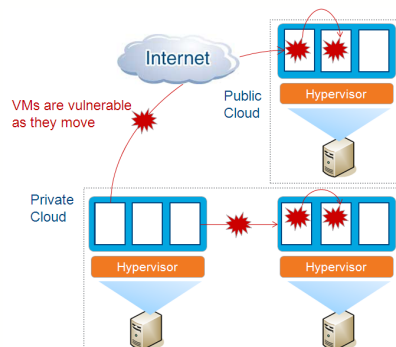
Los equipos virtuales son dinámicos: se pueden revertir rápidamente a instancias anteriores, así como pausar y reiniciar con relativa facilidad. También se pueden clonar de inmediato y mover sin fisuras entre servidores físicos. Esta naturaleza dinámica, junto con la capacidad de los equipos virtuales para expandirse, hace que sea difícil conseguir y mantener una seguridad coherente. Las vulnerabilidades o los errores de configuración pueden propagarse de manera imperceptible. Asimismo, resulta complicado mantener en todo momento un registro auditable del estado de seguridad de un equipo virtual. En los entornos de informática en Internet será necesario poder demostrar el estado de seguridad de un sistema, independientemente de su ubicación o proximidad con respecto a otros equipos virtuales potencialmente desprotegidos.

USOS ILEGÍTIMOS DE LAS VULNERABILIDADES Y ATAQUES DE EQUIPO VIRTUAL A EQUIPO VIRTUAL

Los servidores de informática en Internet utilizan los mismos sistemas operativos y aplicaciones Web y empresariales que los equipos virtuales y servidores físicos con ubicación conocida. La habilidad de un atacante o malware para hacer uso ilegítimo de las vulnerabilidades de forma remota en estos sistemas y aplicaciones es una amenaza a tener muy en cuenta en los

"Sería estupendo que este nuevo enfoque de suministro de servicios basados en TI fuera seguro en esencia. Sin embargo, la realidad de los ataques y errores humanos hacen que se necesiten otros controles de seguridad para proteger las empresas de los incidentes de seguridad que surgen como consecuencia de la migración a sistemas informáticos basados en Internet... Si bien será preciso contar con controles de seguridad perimetral para proteger el resto de funciones del centro de datos y a la todavía extensa comunidad de usuarios empresariales que no usa dispositivos móviles, se necesitan nuevos enfoques que garanticen la protección de los servicios de TI basados en Internet."

Gartner, "Cloud-Based Computing Will Enable New Security Services and Endanger Old Ones," junio de 2008



SEGURIDAD DE LA INFORMÁTICA EN INTERNET

PREPARACIÓN DE EQUIPOS VIRTUALES PARA INTERNET

entornos de informática en Internet virtualizados. Además, el hecho de que varios equipos virtuales compartan la misma ubicación aumenta la superficie de ataque y el riesgo de infecciones de un equipo virtual a otro. Los sistemas de detección y prevención de intrusiones deben poder detectar la actividad maliciosa en el nivel de equipo virtual, sin que importe dónde se encuentre éste dentro del entorno público virtualizado.

PROTECCIÓN DE EQUIPOS VIRTUALES INACTIVOS

Al contrario de lo que sucede con los equipos físicos, cuando un equipo virtual se desconecta, sigue estando disponible para cualquier aplicación que tenga acceso al almacén de equipos virtuales a través de la red y, por tanto, es susceptible de sufrir una infección por malware. El problema es que los equipos virtuales inactivos o desconectados no pueden ejecutar un agente de exploración antimalware. Los equipos virtuales inactivos pueden existir en otras ubicaciones además de en el hipervisor y, asimismo, se pueden almacenar en otros servidores o medios de almacenamiento o hacer una copia de seguridad de ellos. En los entornos de informática en Internet, la responsabilidad de la protección y exploración de los equipos inactivos reside en el proveedor de Internet. Por lo tanto, las empresas que usen la informática en Internet deben buscar un proveedor de este servicio que ofrezca protección para los equipos virtuales inactivos y mantenga una seguridad uniforme en todo Internet.

IMPACTO EN EL RENDIMIENTO DE LA SEGURIDAD TRADICIONAL

Las soluciones de seguridad de contenido existentes se crearon antes de que aparecieran los conceptos de virtualización de x86 e informática en Internet y, en consecuencia, no se diseñaron para funcionar en entornos de Internet. En un entorno de Internet, donde los equipos virtuales de distintas empresas comparten los recursos de hardware, las exploraciones de sistema completo simultáneas pueden provocar una reducción del rendimiento en el equipo host subyacente. Los proveedores del servicio de Internet que proporcionan una línea base de seguridad a los clientes que alojan pueden hacer frente a este problema llevando a cabo las exploraciones que conllevan un gran consumo de recursos en el nivel del hipervisor, ya que así se pone fin a esta disputa en el nivel del host.

INTEGRIDAD DE LOS DATOS: UBICACIÓN COMPARTIDA, RIESGOS Y ROBO

Según arroja el informe *Data Breach Investigations Report* realizado en 2008 por el Risk Team de Verizon Business, el 59% de las filtraciones de datos se produjo a causa de las actividades de hackers e intrusiones. Previsiblemente, los recursos dedicados ofrecerán una mayor seguridad que los recursos compartidos. La superficie de ataque en los entornos en Internet compartidos parcial o completamente es, en teoría, más extensa, de modo que el riesgo es también mayor. Por ello, las empresas necesitan seguridad y pruebas auditables de que los recursos en Internet no se alteran ni se ponen en riesgo, especialmente si éstos residen en una infraestructura física compartida. El sistema operativo y los archivos y actividades de las aplicaciones se deben supervisar.

CIFRADO Y PROTECCIÓN DE DATOS

Existe un gran número de normativas y estándares, como PCI DSS y HIPAA, que incluye requisitos en cuanto al uso del cifrado para proteger la información confidencial (por ejemplo, los datos del titular de una tarjeta o la información personal identificable) a fin de cumplir con las normativas o disponer de un lugar seguro en caso de que se produzca una filtración. La esencia multiempresarial (*multi-tenant*) de los entornos en Internet supone un aumento de estos requisitos y plantea retos nunca antes vistos en relación con la accesibilidad y protección de las credenciales de cifrado que se usan para garantizar la protección de los datos.

GESTIÓN DE PARCHES

La naturaleza de autoservicio de la informática en Internet puede generar confusión a la hora de distribuir esfuerzos para gestionar los parches. Cuando una empresa se suscribe a un recurso de informática en Internet (por ejemplo, al crear un servidor Web a partir de las plantillas que proporciona el proveedor de servicio de informática en Internet de turno), la gestión de parches correspondiente a dicho servidor ya no corre a cargo del proveedor, sino que pasa a manos del suscriptor. Teniendo en cuenta que, según el informe de Verizon mencionado anteriormente, para el 90% de las vulnerabilidades conocidas que los atacantes aprovecharon existían parches seis meses antes de que se produjera la violación en cuestión, las organizaciones que usan la informática en Internet deben estar alerta para actualizar los recursos de Internet con los últimos parches que el proveedor haya puesto a disposición. Si la aplicación de parches no es posible o no se puede gestionar, deberá considerarse la posibilidad de implementar controles de compensación, como la “aplicación de parches virtuales”.

“Para el 90% de las vulnerabilidades conocidas que los atacantes aprovecharon ya existían parches seis meses antes de que se produjera la violación.”

Informe *Data Breach Investigations Report* de 2008
Risk Team de Verizon Business

POLÍTICAS Y CUMPLIMIENTO

Las empresas se encuentran sometidas a una enorme presión para cumplir una amplia gama de normativas y estándares, como PCI, HIPAA y GLBA, además de otras tantas prácticas de auditoría como SAS70 e ISO. En este sentido, deben probar el cumplimiento con estándares de seguridad, independientemente de dónde se encuentren los sistemas sujetos a dichas normativas, ya sea en servidores físicos in situ, equipos virtuales in situ o equipos virtuales externos que se ejecutan en recursos de informática en Internet.

PROTECCIÓN PERIMETRAL Y ZONAS

En la informática en Internet, el perímetro de la red empresarial se evapora y hasta el más mínimo denominador común tiene impacto en la seguridad global. El cortafuegos de la empresa, que es la base para establecer políticas de seguridad y zonas en las redes, no puede tener acceso a los servidores de informática en Internet, o bien el control de las políticas no recae en el propietario del recurso, sino en el proveedor de la informática en Internet. Para establecer zonas de confianza en Internet, los equipos virtuales deben disponer de autodefensa, con lo cual el perímetro se desplaza eficazmente al propio equipo virtual.

“... nuestros clientes ya no nos necesitan para adquirir y usar estas nuevas tecnologías. Sin embargo, el verdadero poder de los CIO reside en su capacidad de ayudar a la organización y a los clientes a usar estas tecnologías para siempre.”

Linda Cureton, CIO, NASA,
Centro aeroespacial Goddard Space
Flight Center

RECURSOS EMPRESARIALES MALICIOSOS

Ansiosos por disponer de recursos y resultados informáticos inmediatos, son muchos los usuarios y grupos con escasos conocimientos de TI que se están subiendo al carro de la informática en Internet. Los datos y aplicaciones empresariales importantes se implementan en Internet, probablemente sin tener en cuenta ninguna implicación de seguridad.

V. PREPARACIÓN DE EQUIPOS VIRTUALES PARA INTERNET

La virtualización es la tecnología que hace posible la informática en Internet. Aquellas organizaciones que no estén utilizando la informática en Internet hoy día muy probablemente lo harán en el futuro. Los centros de datos que han consolidado los servidores físicos en varias instancias de equipo virtual en servidores virtualizados pueden llevar a cabo los pasos inmediatos necesarios para aumentar la seguridad en el entorno virtualizado, así como preparar a dichos equipos virtuales para migrarlos a entornos en Internet, si procede.

A continuación se describen cinco tecnologías de seguridad (cortafuegos, detección y prevención de intrusiones, supervisión de integridad, inspección de registros y protección frente a malware) que se pueden implementar como software en equipos virtuales para aumentar la protección y mantener la integridad del cumplimiento de servidores y aplicaciones a medida que los recursos virtuales se trasladan de instalaciones in situ a entornos de Internet públicos.

CORTAFUEGOS

Disminución de la superficie de ataque de los servidores virtualizados en entornos de informática en Internet.

Un cortafuegos de inspección de estado bidireccional implementado en los equipos virtuales individuales proporciona una gestión centralizada de las políticas de cortafuegos del servidor, que incluye las plantillas predefinidas para tipos comunes de servidores empresariales y permite lo siguiente:

- Aislamiento de los equipos virtuales
- Filtrado avanzado (direcciones de origen y de destino, puertos)
- Cobertura de todos los protocolos basados en IP (TCP, UDP, ICMP, etc.)
- Cobertura de todos los tipos de trama (IP, ARP, etc.)
- Prevención frente a ataques de denegación de servicio (DoS)
- Posibilidad de diseñar políticas de diseño por interfaz de red
- Detección de exploraciones de reconocimiento en servidores de informática en Internet
- Notificación de ubicaciones para lograr una política estricta y la flexibilidad para mover el equipo virtual de la instalación in situ a los recursos en Internet

SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

Protección de las vulnerabilidades de los sistemas operativos y las aplicaciones empresariales hasta que se les puedan aplicar parches para obtener la protección oportuna frente a los ataques conocidos y de día cero.

Tal y como se ha indicado anteriormente, los equipos virtuales y los servidores de informática en Internet utilizan los mismos sistemas operativos y aplicaciones Web y empresariales que los servidores físicos. La implementación de la detección y prevención de intrusiones a modo de software en los equipos virtuales protege de las vulnerabilidades recientemente descubiertas en dichas aplicaciones y sistemas operativos para, así, proporcionar protección frente a los ataques que ponen en riesgo a los equipos virtuales. En concreto, las reglas de vulnerabilidad protegen las vulnerabilidades conocidas, por ejemplo, aquellas que Microsoft revela mensualmente, de una serie ilimitada de amenazas.

SUPERVISIÓN DE INTEGRIDAD

Supervisión de los archivos, los sistemas y el registro en busca de cambios.

La supervisión de integridad de los sistemas operativos y archivos de aplicación esenciales (archivos, directorios, claves de registro, valores, etc.) es necesaria para detectar cambios maliciosos e inesperados indicativos de un riesgo en los recursos de informática en Internet. El software de supervisión de integridad se debe aplicar en el nivel de equipo virtual.

Una solución de supervisión de integridad debería permitir lo siguiente:

- Detección bajo petición o programada
- Comprobación completa de propiedad de archivos, incluidos los atributos (permite el cumplimiento con PCI 10.5.5)
- Supervisión en el nivel de directorio
- Supervisión flexible y práctica mediante inclusión/exclusión
- Informes de auditoría

INSPECCIÓN DE REGISTROS

Visibilidad de eventos de seguridad importantes escondidos en archivos de registro en los recursos de Internet.

La inspección de registros recopila y analiza sistemas operativos y registros de aplicaciones en busca de eventos de seguridad. Las reglas de inspección de registros optimizan la identificación de eventos de seguridad importantes escondidos en múltiples entradas del registro. Si bien estos eventos se pueden enviar a un sistema de seguridad independiente, logrará la máxima visibilidad si se reenvían a un sistema de gestión de información de seguridad y eventos (SIEM) o a un servidor de registro centralizado para la correlación, generación de informes y archivado. Al igual que la supervisión de integridad, las funciones de la inspección de registros se deben aplicar en el nivel de equipo virtual. El software de inspección de registros en los recursos de Internet permite lo siguiente:

- Detección de comportamiento sospechoso
- Recopilación de acciones administrativas relacionadas con la seguridad
- Recopilación optimizada de eventos de seguridad del centro de datos

PROTECCIÓN ANTIMALWARE CON CAPACIDAD DE VIRTUALIZACIÓN

Cierre de las brechas de seguridad exclusivas de los entornos virtuales y de Internet.

La protección antimalware con capacidad de virtualización aprovecha las API de introspección del hipervisor (como las API de VMware VMsafe) para proteger los equipos virtuales tanto activos como inactivos. La protección multicapa utiliza equipos virtuales especializados de exploración coordinados con agentes en tiempo real en cada equipo virtual. Así, se garantiza la seguridad de los equipos virtuales cuando están en estado de inactividad y la protección mediante las actualizaciones de patrones más recientes cuando se activan. Asimismo, la protección antimalware con capacidad de virtualización puede conservar el perfil de rendimiento de los servidores virtuales cuando se ejecutan operaciones que requieren un gran consumo de recursos (por ejemplo, las exploraciones completas del sistema desde un equipo virtual de exploración distinto).

- Nulo impacto del malware en los equipos virtuales activos e inactivos
- Protección frente a ataques que desinstalan, frenan o revisan de forma fraudulenta la seguridad antivirus
- Estrecha integración con las consolas de gestión de la virtualización, como VMware vCenter
- Configuración automática de la seguridad de los nuevos equipos virtuales

CONSIDERACIONES SOBRE LA IMPLEMENTACIÓN DE SEGURIDAD

Con el tiempo, los entornos de informática en Internet van a protagonizar un enorme aumento. Los equipos virtuales de los entornos en los que se implementan los mecanismos de seguridad antes mencionados estarán perfectamente preparados para Internet. Existen tres consideraciones adicionales que contribuyen a maximizar la eficacia de cualquier implementación de seguridad:

- Los agentes de software de los equipos virtuales confieren una mayor seguridad a estos equipos. La consolidación de los mecanismos de protección dará pie a economías de escala, implementación y, en última instancia, un ahorro de costes notable a empresas y proveedores de servicios.
- Probablemente, las empresas no trasladen la totalidad de su informática a los recursos de Internet. En consecuencia, los mecanismos de seguridad deberán ser coherentes en todas las instancias (físicas, virtuales y de informática en Internet) de los servidores y aplicaciones. Asimismo, estas implementaciones deberían poder gestionarse centralmente y permitir la integración con inversiones infraestructurales de seguridad existentes, como las herramientas de integración virtuales (VMware vCenter, por ejemplo), las soluciones de gestión de información de seguridad y eventos (como ArcSight, NetIQ y RSA Envision), los directorios empresariales (Active Directory) y los mecanismos de distribución de software (como Microsoft SMS, Novel Zenworks y Altiris).
- Muchas de las herramientas implementadas actualmente, como el software del cortafuegos o los sistemas de prevención de intrusiones basados en host (HIPS), pueden migrar perfectamente a los entornos de Internet. Además, las herramientas y software gratuitos, como VM Protection, están disponibles para su implementación en entornos virtuales y de Internet.

VI. EMPIECE HOY MISMO

Al igual que todas las variaciones de informática que la han precedido, la informática en Internet conlleva diversos riesgos y desafíos de seguridad, lo cual no significa que su implementación se deba evitar o posponer, ya que las ventajas que resultan de su uso son demasiado buenas como para renunciar a ella.

En tanto que empresa que investiga la informática en Internet, revise los desafíos de seguridad descritos en el presente artículo y sopesa los siguientes interrogantes:

- ¿Usa su organización la informática en Internet actualmente? ¿Son esas aplicaciones o datos implementados fundamentales para la continuidad del negocio? ¿Cumplen o infringen alguna política de seguridad empresarial vigente? ¿Son motivo de una exposición innecesaria de los recursos empresariales existentes?
- ¿Qué mecanismos de seguridad existentes actualmente en la red empresarial no se van a migrar a Internet y qué riesgo supone esto?
- ¿Qué plataforma de virtualización ofrece el proveedor del servicio de informática en Internet escogido? ¿Permite que la empresa mueva recursos de forma segura y libre hacia y desde Internet?
- ¿Qué software de seguridad se puede utilizar para conseguir la protección suficiente para trasladar los equipos virtuales a los entornos en Internet? Las herramientas de software como VM Protection permiten que las empresas dispongan rápidamente de una línea de defensa para los recursos de informática en Internet.

En cuando a los proveedores del servicio de informática en Internet, considere lo siguiente:

- ¿Está la plataforma de virtualización preparada para aceptar equipos virtuales existentes procedentes de los clientes de la empresa que migran los recursos existentes a nuestros entornos en Internet?
- ¿Cómo ayudamos a los clientes a cumplir los requisitos de zonas y segregación en los recursos de nuestros entornos en Internet mientras mantenemos el coste total de la propiedad más bajo al maximizar las ventajas de disponer de recursos virtuales totalmente compartidos?
- ¿Qué mecanismos de seguridad podemos implementar o recomendar para que los equipos virtuales de nuestros clientes puedan estar preparados para Internet?

VII. RESUMEN

Los proveedores del servicio de informática en Internet sacan partido de las tecnologías de virtualización combinadas con una serie de funciones de autoservicio para proporcionar un acceso rentable a los recursos informáticos a través de Internet. Para que los proveedores del servicio de informática en Internet aprovechen al máximo la eficacia de la virtualización, los equipos virtuales de varias organizaciones deberán residir conjuntamente en los mismos recursos físicos. Aquellas empresas que recurren a la informática en Internet para ampliar la infraestructura in situ deben ser conscientes de los retos de seguridad que pueden poner en peligro la integridad del cumplimiento y la seguridad de sus aplicaciones y datos.

La extensión de los equipos virtuales a las redes públicas hace que el perímetro de la red empresarial se evapore y que hasta el más mínimo denominador común tenga impacto en la seguridad global. La incapacidad de la seguridad basada en el hardware y la segregación física de hacer frente los ataques entre los equipos virtuales en el mismo servidor acucia la necesidad de disponer de mecanismos que se implementen directamente en el servidor o en los equipos virtuales.

Por lo tanto, la implementación de una línea de defensa que incluya cortafuegos, detección y prevención de intrusiones, supervisión de integridad, inspección de registros y protección frente a malware como software en los equipos virtuales será el método más eficaz para mantener la integridad del cumplimiento y conservar la protección de las políticas de seguridad a medida que los recursos virtuales se trasladan de instalaciones in situ a entornos de Internet públicos. Las empresas y los proveedores de servicio previsoros ya están aplicando esta protección en los equipos virtuales con el propósito de obtener una seguridad preparada para Internet y, de este modo, poder aventajar a la competencia en el uso de la informática en Internet.

Para obtener más información, puede llamarnos o visitarnos en:
<http://es.trendmicro.com/es/home/enterprise/>