RESPUESTAS SIC

Madrid: 14 de octubre de 2008
(Hotel NH Eurobuilding)

Barcelona: 17 de octubre de 2008
(Hotel Rey Juan Carlos I)

Eficiencia y protección sin fisuras

El reto de la virtualización segura

Inscripciones:

- Acceso gratuito previa solicitud de inscripción.
- Solicitud: www.revistasic.com/respuestassic

> AFORO LIMITADO

Copatrocinan:

FORTINET McAfee STONESOFT symantec. TREND MICRO

Organiza:

Revista SIC seguridad en informática y comunicaciones

El reto de la virtualización

El uso generalizado de la virtualización (servidores, aplicaciones, almacenamiento, redes...), pudiera ser una de las grandes revoluciones en el sector de las tecnologías y los sistemas empresariales. Bajo ciertas condiciones representa una oportunidad atractiva para racionalizar y optimizar recursos, consolidar infraestructuras completas, incrementar la flexibilidad y la agilidad en la prestación de servicios, y obtener mejoras en algunos frentes de la protección de la información.

Sin embargo, como todo factor nuevo que entra a formar parte del sistema tecnológico de una entidad, es menester realizar un análisis pormenorizado de la tipología de los riesgos que acarrea su despliegue en los distintos escenarios y, particularmente, de los cambios que puede provocar su uso en los modelos "tradicionales" de administración de seguridad.

Y es que, en efecto, muchos especialistas coinciden en que la aplicación de la virtualización en la operación de la seguridad TIC tendrá un impacto notable en los modelos ya instaurados en las organizaciones, en orden a conseguir una protección unificada y eficiente de la información en los sistemas, los "físicos" y los "virtualizados". Al tiempo, se acentuará la necesidad de conocer y clasificar la información corporativa crítica y de valor, y de implantar medidas estrictas de control ante la posibilidad de migrar con rapidez máquinas virtuales entre *hosts*.

Así pues, en esta sesión de Respuestas SIC –dedicada a un campo de notable atractivo, que despierta numerosas incertidumbres y en el que los fabricantes específicos van a tener que aplicarse a fondo–, además de evidenciar las

Percepciones y tendencias

Percepción de los riesgos de seguridad en máquinas virtuales

Fuente: InformationWeek Analytics-VMware Security Survey 2008. A partir de las respuestas de 423 profesionales

¿Quién es el responsable de garantizar que los servidores virtuales estén configurados de forma segura?

	Administradores de Sistemas	Director de Operaciones	Seguridad	Nadie	Otros
Operaciones	57%	14%	17%	3%	8%
Seguridad	47%	11%	37%	0%	5%
Cumplimiento	20%	40%	0%	0%	40%
Arquitectura de TI	38%	8%	54%	0%	0%
Otros	58%	8%	33%	0%	0%
Total de respuestas	49%	13%	31%	1%	6%

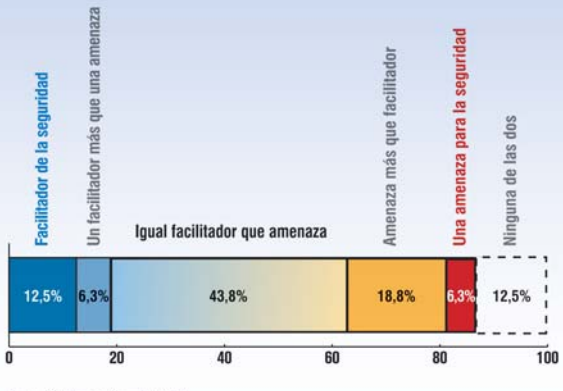
Fuente: Informe de Tripwire 2008: "Is Virtualization Under Control?"

Abordando los retos de seguridad en entornos virtuales

54%	Uso de herramientas tradicionales de seguridad de infraestructura (cortafuegos, monitorización de red, sistemas de detección de intrusos, antivirus, NAC, etc.) **sin provisión específica para virtualización**
17%	Uso de herramientas tradicionales de seguridad de infraestructura (cortafuegos, monitorización de red, sistemas de detección de intrusos, antivirus, NAC, etc.) **con módulos de virtualización o *plug-ins***
12%	Uso de herramientas específicas de seguridad para virtualización **proporcionadas por un fabricante de virtualización para la gestión de la seguridad en entornos virtuales, de forma añadida a otras herramientas tradicionales de protección**
3%	Uso de **herramientas de seguridad de terceros diseñadas para máquinas virtuales** (*appliances* de seguridad virtual, IDS) para gestionar la protección en entornos virtuales y en entornos tradicionales
2%	Uso de herramientas de seguridad de terceros solo para virtualización (*appliance* de seguridad virtual, IDS o monitores intra-*host* para máquinas virtuales) **para gestionar la seguridad en entornos virtuales de forma añadida a herramientas de seguridad tradicional**
12%	**Sin provision de seguridad** para máquinas virtuales

Fuente: InformationWeek Analytics-VMware Security Survey 2008. A partir de las respuestas de 423 profesionales

¿En su opinion, la virtualización del servidor es un facilitador de la seguridad o una amenaza para la seguridad?



Fuente: CSI-Computer Security Institute

ventajas que la técnica objeto de debate pudiera aportar a la mejora de la seguridad, se realizará una puesta al día de la situación evolutiva de las soluciones tecnológicas que la industria especializada en protección de la información, muy activa en este emergente segmento, propone para gestionar los riesgos asociados al uso de la virtualización.

Contenido

Como viene siendo habitual, la sesión se dividirá en tres bloques: en el primero, y mediante la intervención de un consultor especializado –en este caso de la compañía **Germinus (Grupo Gesfor)**–, se llevará a cabo un acercamiento a la realidad tecnológica y a los retos de administración y control al optarse por esta alternativa.

A continuación tendrá lugar un segundo bloque, en el que especialistas de las compañías **Fortinet**, **McAfee**, **Stonesoft**, **Symantec** y **Trend Micro** expondrán sintéticamente las características más relevantes de sus soluciones para proteger los escenarios virtualizados.

Finalmente, el tercer y último bloque lo conformará una mesa redonda en la que tres expertos en seguridad TIC de **CTTI-Generalitat de Cataluña**, **Grupo BBVA** y **Telefónica** brindarán su opinión profesional acerca del tema nuclear de esta jornada.

Programa

CLAVES PARA DECIDIR

09:00h. Acreditación y entrega de documentación.

09:30h. **El reto de la virtualización segura: estrategias y estado del arte**

Ponente: **Javier Fernández-Sanguino**,
Responsable de la División de Seguridad Lógica de Germinus (Grupo Gesfor).

10:20h. Coloquio.

APROXIMACIONES DE LA INDUSTRIA

10:25h. **Fortinet**.

Emilio Román,
Director General.

10:45h. **McAfee**.

Blas Simarro Lorite,
Director Técnico.

11:05h. **Stonesoft**.

María Campos Sánchez,
Directora General.

11:25h. Pausa-café.

11:55h. **Symantec**.

Javier Ferruz Rodríguez,
Consultor Senior Preventa.

12:15h. **Trend Micro**.

Gabriel Agatiello,
Responsable de Producto.

12:35h. Coloquio general.

MESA REDONDA

13:00h. **La visión de los usuarios. Escenarios actuales, limitaciones y necesidades futuras.**
Participantes:

Tomás Roy Catalá,
Director del Área de Calidad, Seguridad y Relaciones con Proveedores.
CTTI – Generalitat de Cataluña.

Carlos Pérez Navarro,
Responsable de Ingeniería de Seguridad.
Dirección de Seguridad Lógica.
Grupo BBVA.

Juan Miguel Velasco López-Urda,
Director Asociado de Servicios de Seguridad y Proyectos de Seguridad de la Unidad de Grandes Clientes de Telefónica España. **Telefónica.**

14:30h. Almuerzo para todos los asistentes.

* Revista SIC se reserva el derecho a modificar el contenido o los ponentes de este programa si las circunstancias así lo requieren.

Eficiencia y protección sin fisuras

"Los entornos de virtualización introducen nuevos elementos de gestión a los elementos de gestión tradicionales de sistemas. Desde estos elementos de gestión, se puede llevar a cabo la asignación de recursos y dispositivos de los sistemas virtualizados, acciones sobre los sistemas (como el apagado y el encendido) y el acceso a la consola de los equipos".

Javier Fernández-Sanguino
(Revista SIC nº 77)

Hacia una virtualización segura de las infraestructuras

Cada año los responsables de seguridad de la información tienen que enfrentarse a la última moda en tecnología de sistemas de información, estudiarla, comprenderla y decidir qué recomendaciones deben dar para su adecuado despliegue y correcta utilización. Este artículo aborda una de las palabras de moda: la *virtualización*, y en él se presta es[illegible]ción a la consoli-d[illegible]uras

- ¿Cuáles son las mejoras en materia de seguridad de la información que puede aportar la virtualización?
- ¿Qué consecuencias tiene en el modelo de administración de la seguridad TIC de una organización la aplicación de la virtualización?
- ¿Cuándo se puede afirmar que el coste de la seguridad de los sistemas "virtualizados" es inferior al de los sistemas "físicos"?
- ¿Qué efectos pueden esperarse del uso de la virtualización en las unidades que tienen la responsabilidad de la detección, análisis y obtención de evidencias digitales?
- ¿Están preparados los departamentos de sistemas y las unidades de seguridad TIC para gestionar los riesgos asociados al cambio constante que podría permitir un uso poco controlado de la virtualización en ciertos entornos, esenciales para sustentar procesos de negocio en sus organizaciones?
- ¿Aumentará en el futuro el número de vulnerabilidades de los productos de virtualización?
- En atención al tipo de información que manejen, ¿es necesario que exista en el desarrollo normativo de la política de seguridad TIC de la empresa una indicación en la que se estipule qué máquinas virtuales pueden o no compartir el mismo hardware?
- ¿A qué retos se enfrenta la industria especializada en protección TIC para ofrecer herramientas tecnológicas que ayuden a operar de modo cada vez más eficiente la seguridad de los sistemas virtualizados y físicos?
- ¿Qué impacto tendrá en el control de la seguridad de la información de una organización la contratación de servicios externalizados a prestadores con entornos crecientemente virtualizados?
- ¿Son suficientemente atractivos los entornos virtualizados como para estimular la aparición de código malicioso especializado?
- ¿Cómo se espera que afronten hoy los departamentos de auditoría la revisión del impacto en la seguridad de la información del uso creciente de la virtualización en el sistema tecnológico de sus organizaciones?
- ¿Qué impacto tiene la virtualización en los procesos de almacenamiento, recuperación y *backup* de la información?

RESPUESTAS SIC

El reto de la virtualización segura

LUGAR Y FECHAS

- **MADRID: 14 de octubre de 2008**
  Hotel NH Eurobuilding.
  C/. Padre Damián, 23. 28036 Madrid
- **BARCELONA: 17 de octubre de 2008**
  Hotel Rey Juan Carlos I.
  Avda. Diagonal, 661-671. 08028 Barcelona

ORGANIZA

Revista SIC. Ediciones CODA.
C/. Goya, 39. 28001 Madrid
Tel.: 91 575 83 24
info@revistasic.com www.revistasic.com

SOLICITUD DE INSCRIPCIÓN GRATUITA

El procedimiento para la solicitud de la inscripción es vía web mediante la cumplimentación de un formulario. Al ser el aforo limitado, la inscripción se cursará por riguroso orden de fecha de entrada de solicitud.

Sitio web: www.revistasic.com/respuestassic

- Una vez realizada la solicitud, la organización le informará –por razones de limitación del aforo– si ha quedado inscrito o no.
- En ningún caso se admitirán más de dos inscripciones de profesionales de una misma compañía.
- La sesión incluye documentación, café y almuerzo.