



## Virtualización: Implicancias de la seguridad de la información

Autor: Fernando Sanchez – [fsanchez@cybsec.com](mailto:fsanchez@cybsec.com)

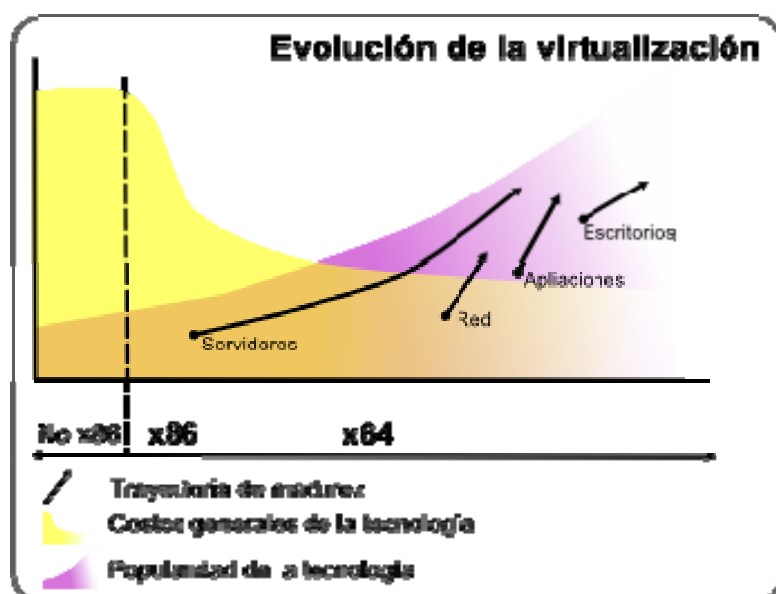
En estos últimos años la tecnología de virtualización ha evolucionado alcanzándose una madurez interesante en esta tecnología, no solo técnicamente, superando la “tradicional” línea de virtualización de servidores e incorporando nuevas funcionalidades, sino que también, en lo que a herramientas para la gestión de recursos y procesos asociados a ellas se refiere.

Este nivel de maduración, las crecientes capacidades del hardware que soporta a la virtualización y, principalmente, las muchas ventajas que genera para la gestión de IT y la baja de costos que conlleva, han hecho que esta tecnología logre un alto nivel de popularidad en las áreas de IT de cualquier industria.

Pero no todo es color de rosa en el mundo de la virtualización. Hay aspectos, que por maximizar las principales ventajas, no se toman en cuenta o no se valorizan correctamente y que pueden llegar a generar huecos de seguridad para los activos de IT de nuestra organización.

Una de estas brechas de seguridad es, lo que se puede denominar

como, la homogenización física de los niveles de seguridad de los diferentes ambientes, es decir:



En la actualidad, una organización que aplique buenas prácticas de seguridad de la información, poseerá varios ambientes con mayores o menores restricciones para acceder a la información, uno para el desarrollo de aplicaciones (Desarrollo), otro para la prueba de los sistemas desarrollados (Testing), otro para los sistemas que prestan servicio a los usuarios finales (Producción), uno más que presta servicios públicos (DMZ) y por último el ambiente del usuario final (Escritorios). Hoy en día, técnicamente, todos estos ambientes pueden ser soportados por una misma infraestructura física e hipervisor<sup>1</sup>; pero esta homogenización física eleva el riesgo de

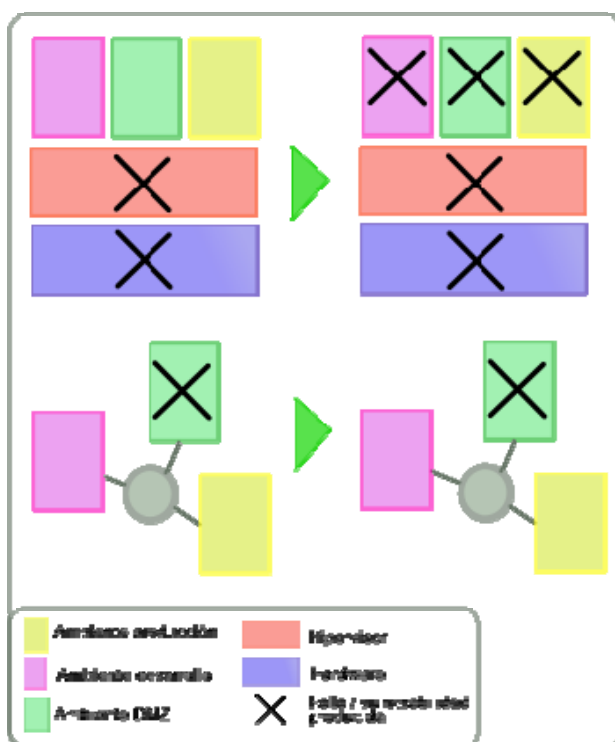
<sup>1</sup> **Hipervisor:** Un hipervisor (en inglés *hypervisor*) o monitor de máquina virtual (*virtual machine monitor*) es una plataforma de virtualización que permite utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora. (fuente: <http://es.wikipedia.org/wiki/Hypervisor>)



sobrepasar cada una de las restricciones de seguridad propias de cada ambiente que han sido definidas ya sea, por motus propio, por seguimiento de buenas prácticas de seguridad de la información por parte de la dirección o por necesidad de cumplir con regulaciones nacionales o internacionales.

Esta homogenización física de la que hablamos genera un riesgo, dado que en caso de un compromiso de la infraestructura de virtualización, se expone a los servidores atendidos por ella y le permitiría a un intruso, a través de la ejecución de vulnerabilidades conocidas y públicas, acceder a la información contenida en ellos o tomar su control. Y considerando que, hoy en día, si se tiene correctamente protegido el borde de la red y los servicios publicados, la mayoría de las intrusiones provienen del interior de la organización y de personas que tienen conocimiento e

incluso credenciales para acceder a los sistemas de la organización y hasta, en algunos casos, con privilegios elevados, el riesgo de homogenizar el nivel de seguridad de los diferentes ambientes debe ser considerado seriamente.



Otra potencial brecha de seguridad, es el compromiso del hipervisor a través del compromiso del equipo virtualizado. Si bien hasta el momento no se conoce la existencia de vulnerabilidades, en este sentido hay dos posiciones casi encontradas, por un lado los defensores de la virtualización que establecen que esta brecha sería prácticamente inexistente, dado que habría que saltar los controles y barreras de protección del sistema operativo virtualizado, altamente probadas en el ambiente físico; por ejemplo el sistema operativo

virtualizado, que tiene asignado 1Gb de memoria RAM, no conoce que en realidad la memoria RAM es de 8Gb. Y por el otro lado se encuentran los que consideran que es cuestión de tiempo, y de prueba y error, el que se publiquen vulnerabilidades en este sentido, dado que en esta tecnología existe lo que se denomina vectores de ataque<sup>2</sup>, que podrían llegar a ser utilizados para comprometer el hipervisor a través del sistema operativo virtualizado, como ser las herramientas que permiten la interacción directa entre el servidor físico y el virtual, algunas de ellas, “VMware tools” de VMware o las “guest addition” de virtualbox.

Más allá de las vulnerabilidades que cada una de las tecnologías de virtualización podría llegar a poseer, existen riesgos a considerar que están relacionadas con los

<sup>2</sup> **Vector de ataque:** Un vector de ataque es una ruta o un medio que un intruso puede utilizar para acceder o comprometer a un servidor o servicio.



recursos que dan soporte a la infraestructura de virtualización, tanto humanos como de hardware, como ser:

- La concentración de las fallas en la gestión de la misma, que si bien, también pueden producirse en el ambiente físico, el alcance e impacto de estas fallas cobra mayor relevancia dado que puede afectar a varios equipos a la vez, ya que se tienen todos los equipos en una misma infraestructura y consola de administración.
- Otro riesgo destacable a considerar, en particular para un ambiente de virtualización, son las medidas de seguridad necesarias para mitigar los riesgos por disponibilidad del servicio, dado que los servidores, el almacenamiento y las comunicaciones que soportan el ambiente de virtualización pasan a ser críticos para la organización y el solo hecho de que se acabe el almacenamiento podría llegar a generar una denegación de servicio sobre todos los servidores y dispositivos virtualizados.

Por otro lado, la tecnología de virtualización correctamente implementada le acerca al mundo de la seguridad informática herramientas que permiten agilizar las soluciones a varias problemáticas, en particular, las asociadas a la disponibilidad de los servicios e información. En este sentido facilita los procesos para realizar copias de respaldo, ya que la información se encuentra concentrada en un menor número de locaciones, también los procesos de los DRPs y BCPs dado que los servidores que soportan las aplicaciones del negocio no dependen del hardware, permitiendo que fácilmente puedan ser migrados a otra locación.

Aplicando las correctas medidas de seguridad, tanto lógicas como físicas, sobre los servidores que soportarán al hipervisor y sus herramientas de administración y sobre los equipos virtualizados y de comunicaciones involucrados y en definitiva en toda la solución de virtualización, es posible sacarle provecho a las ventajas que aporta esta tecnología no solo sin rescindir los niveles de seguridad actuales, sino que, incluso facilitando el alcanzar mayores niveles de madurez en lo que a seguridad de la información respecta.