

## **Seguridad de la computación en la nube: el Hipervisor**

Recientemente se ha publicado un informe de la Cloud Security Alliance en el que se destacan las principales amenazas o problemas de seguridad que se pueden encontrar en la utilización de la computación en la nube (también conocida por su sinónimo en inglés *Cloud Computing*).

Como ustedes sabrán, la computación en la nube se basa en la externalización de toda la infraestructura utilizada por la empresa en sus procesos informáticos, de forma que un proveedor de servicios mantiene tanto el *hardware* como el software necesario, y proporciona al usuario un punto de acceso a toda esa infraestructura.

Como mantener una infraestructura separada para cada cliente es muy costoso, las empresas que proporcionan este tipo de servicios (llamados *Infrastructure as a Service*, o IaaS) utilizan técnicas de virtualización para rebajar costes y aumentar las posibilidades de escalado de sus sistemas. La virtualización permite en este caso compartir recursos del proveedor entre varios clientes. Pero estos recursos no suelen estar preparados para soportar los niveles de aislamiento requeridos por las tecnologías actuales de virtualización. Para salvar este bache y controlar los recursos que se asignan a cada cliente, los entornos de virtualización disponen de un sistema (llamado Hipervisor) que actúa de mediador entre los sistemas virtuales de los clientes y el sistema principal.

Este hipervisor añade otra capa de abstracción, lo que genera un punto de fallo más además de los puntos de fallo en aplicaciones y sistemas operativos controlados habitualmente. Pero lo importante de este punto de fallo es su criticidad, ya que podría permitir puentear el hipervisor y acceder de forma directa a la infraestructura física, obteniendo acceso a todos los datos del equipo físico (incluidos datos de otros clientes). Esto ya ha sido demostrado anteriormente, con los prototipos de malware llamados *Red Pill* y *Blue Pill* de Joanna Rutkowska, y en las conferencias BlackHat de los años 2008 y 2009.

Una vez conocido este problema y la amenaza que supone para la seguridad de nuestros datos, el siguiente paso consiste en mitigarlo. En esta línea se pueden realizar las siguientes acciones:

- Implementar sistemas de “mejores prácticas” de seguridad durante la instalación y configuración de los sistemas y aplicaciones.

- Llevar un control exhaustivo del entorno para detectar actividades y cambios no autorizados tanto en las tareas y procesos habituales como en los datos almacenados en los sistemas virtualizados.
- Promover controles de autenticación y acceso muy estrictos para el acceso y realización de operaciones administrativas.
- Implantar de Acuerdos de Nivel de Servicio (SLA) para la aplicación de parches y corrección de vulnerabilidades.
- Realizar análisis de vulnerabilidades y auditorías de la configuración de forma periódica.

Para concluir, cabe resaltar la importancia que está cobrando la computación en la nube en estos momentos, con lo cual detectar y solventar estas y otras amenazas es crucial para adaptarse a las necesidades de seguridad del usuario, y dotar al servicio de las garantías necesarias en esta materia.

Fecha: 28/05/2010

Fuente: [securityartwork.es](http://securityartwork.es)