Soluciones IBM para Seguridad en la Nube

Andrés Oswaldo Vega
Especialización en Seguridad de la Información
Universidad Piloto de Colombia
andresvega@misena.edu.co
Bogotá, Colombia

***Abstract*— The present paper is an analysis of the IBM technologies proposed to enforce the information environments based on Cloud Computing, implementing "IBM Endpoint Manager", "IBM Smart Cloud Patching Management", "IBM Smart Cloud Provisioning" and "Intrusion Detection and Prevention System (IDPS) Management", additional is proposed the possibility to use the IBM Framework deployment to secure the multivendor platforms technologies keeping the assessment process.**

***Resumen*— En el presente documento se realiza una análisis de tecnologías propuestas por la empresa IBM para fortalecer los entornos de información basados en "La Nube" mediante la implementación de los aplicativos "IBM Endpoint Manager", "IBM Smart Cloud Patching Management", "IBM Smart Cloud Provisioning" y "Gestión de Sistemas de Detección y Prevención de Intrusos", además se plantea la posibilidad de utilizar el FrameWork desarrollado por IBM para el aseguramiento de tecnologías de diferentes fabricantes siguiendo un proceso de evaluación.**

***Palabras claves* — Cloud Computing, Aseguramiento, Endpoint, Cliente, Servidor, Cifrado, Detección, Virtualización.**

I. Introducción

La seguridad de la información en redes de área amplia se ha convertido en el principal dolor de cabeza para grandes organizaciones que piensan en la nube como una solución a sus problemas, el deseo de lograr servicios que brinden mayor portabilidad y nivel de acceso involucra mayor número de variables que los desarrolladores de aplicaciones antes no tenían que afrontar, la tendencia a extender los servicios de la organización a dispositivos portables generan grandes dudas sobre la efectividad de la aplicación de controles para productos tan variados, IBM en la búsqueda de ofrecer soluciones a estos nuevos retos ofrece varias tecnologías que podrían permitir disminuir el riesgo si estas son correctamente implementadas, además de una estrategia de trabajo en forma de Framework que muestra como enfrentar los problemas de seguridad en entornos Cloud.

II. Manejo simplificado de la seguridad en la nube

A. Retos

A pesar que la tecnología avanza de una manera vertiginosa los modelos de gestión de la información que las empresas poseen cambian con poca velocidad, la adopción de tecnologías en la nube presenta retos específicos para estos modelos de gestión incluyendo el gobierno de la información, control de acceso, monitoreo de la actividad, y visibilidad de recursos, la pregunta que se hacen miles de organizaciones es ¿cómo direccionar todos estos retos de la seguridad de TI en estos entornos tan complejos? [1]

La continuidad en el negocio es un factor fundamental para asumir los riesgos asociados a la computación en la Nube, pero definir una estrategia clara para abarcar un mayor mercado en la cual la organización no se perjudique representa un enorme reto.

B. Enfoque en ambientes virtuales

La evolución los sistemas virtuales ha permitido la masificación de este tipo de tecnologías en el modelo de Cloud Computing por sus siguientes ventajas:

- Bajo costo de licenciamiento.
- Rápido despliegue.
- Menor consumo eléctrico.
- Portabilidad.
- Accesibilidad.

Aunque poseen grandes ventajas, las máquinas virtuales representan un nuevo conjunto de riesgos para las organizaciones por varias razones, por ejemplo, cuando una máquina virtual dura en estado de hibernación o congelamiento mucho tiempo, incluso meses, cuando esta máquina entra en operación no cuenta con la base de datos de virus actualizada, no posee los parches del sistema operativo al día, o las actualizaciones de los aplicativos en el caso de office, flash, java entre los más comunes, generando la exposición de vulnerabilidades conocidas aumentando el nivel de riesgo.

C. "IBM SmartCloud Patch Management"

Es una herramienta que permite la gestión de parches de sistema operativo de forma unificada que provee tres características:

-Soporte para plataformas heterogéneas como Windows, Linux, Unix, Mac Os, etc.
- Evaluación continúa de estado de los parches en las máquinas, incluyendo máquinas virtuales y físicas.
- Nivel de escalamiento y seguridad a nivel de organización, lo que puede brindar granularidad en autorización y capacidad de control de acceso.

La utilización de herramientas como “IBM Smart Cloud”, “Hypervisror”, “VMWARE ESX”, “PowerVm” y “KVM” brindan niveles de control suficientes para disminuir el riesgo a niveles aceptables pero deben ser llevadas de la mano con una certificación EAL 4+ (Evaluation Assurance Level) que garantice la adecuada gestión sobre las herramientas, se debe tener presente que el poder de estas herramientas no solo se basa en la adquisición sino en la correcta implementación y gestión. [2]

D. “IBM SmartCloud Provisioning”

Es una plataforma tipo “Hipervisor” propietaria de IBM similar a Microsoft Hyper-V o VMWare ESX que permite a las empresas adelantarse a las tendencias de la nube permitiendo organizar y en pocas horas aprovisionar una gran cantidad de máquinas virtuales gestionando el almacenamiento, la pre-configuración de imágenes, y la capacidad de crear librerías de máquinas virtuales para una fácil gestión. [3][4]

Esta tecnología logra alta eficiencia eléctrica, alto grado de escalamiento, estandarización de procesos de TI, bajo costo de implementación, balanceo de carga y además de la posibilidad de establecer que configuraciones son inseguras antes de realizar cualquier proceso de despliegue evitando vulnerabilidades antes de que las maquines entren en producción.

E. “Intrusion detection and prevention system (IDPS) management”

En muchas ocasiones la falta de conocimiento asociada a la gestión de complejas herramientas IDPS generan una errónea expectativa frente a la efectividad ofrecida por estos dispositivos, pudiendo generar una falsa sensación de seguridad, o lo contrario, que el dispositivo no está realizando adecuadamente las labores para lo cual fue diseñado, IBM ofrece la posibilidad de realizar la gestión de los IDPS ofreciendo ventajas estratégicas que son difíciles de superar, con la premisa de mantener a los agresores alejados de los activos de la organización, IBM a través de la administración de los IDPS promete la gestión a tiempo de los dispositivos configurando cambios en el menor tiempo posible y utilizando esquemas de “Administración de políticas avanzadas” que permiten la reconfiguración de diferentes dispositivos que estén asociados a la mitigación de algún problema de seguridad.

Las amenazas se pueden detener realizando labores de correlación desde los sistemas de análisis de IBM, los cuales cuentan con información de más de 13 billones de eventos recolectados alrededor del mundo, permitiendo comparar y definir con mayor precisión cuales son las vulnerabilidades que explotara el atacante.[4] [5]

Utilizando algoritmos de inteligencia artificial que han demostrado alta eficiencia se pueden detectar amenazas incluso si son totalmente nuevas, evitando explotaciones de día cero, brindando protección en circunstancias que son imposibles de abordad bajo esquemas de seguridad tradicional.

El sistema de gestión de IDPS de IBM va más allá de detectar situaciones anómalas, sino que realizan cambios en las reglas de los firewalls de forma automática en todos los dispositivos registrados en el portal de administración Web, a través de este portal el contratante podrá ver la identificación de eventos de seguridad registradas por varios dispositivos en una sola interfaz y podrá gestionar cuales dispositivo recibirán las actualizaciones de seguridad recomendadas por IBM.

F. “Endpoint Manager”

Es un potente software que puede ser instalado en prácticamente cualquier sistema final (pcs, tablets, teléfonos, servidores) y permite tener gestión sobre el dispositivo remotamente utilizando un ancho de banda muy bajo, de tal forma que se pueden realizar diagnósticos, gestión de configuraciones, gestión de parches, control de accesos, cifrado de información y borrado de información seguro entre otras posibilidades.

G. FrameWork de gestión de parches.

IBM mediante la investigación que ha realizado en el campo de la gestión de parches de seguridad, IBM ha desarrollado una estrategia sencilla pero que puede ser utilizada en múltiples sistemas de información con posibilidad de adaptación y generar muy buenos resultados.

El proceso está establecido en forma de clico, lo que significa que se retroalimenta cada vez que termina la última etapa.

Las fases del proceso son:

- Evaluación: se realiza una revisión de los productos instalados en el sistema, su versión y estado de licencia comparado con una base de datos que evalúa más de 5000 estados o configuraciones.
- Remediación: se descargan los parches que están disponibles para la máquina y se instalan a través del Empeine Management.
- Fortalecimiento: a través de Endpoint Management se configuran en el sistema diferentes políticas de seguridad que permiten estar protegidos contra las últimas tendencias en intrusión.
- Reporte: utilizando técnicas de análisis de información y gracias al estado de actualización de las bases de datos de IBM se pueden generar reportes de vulnerabilidades por sistema mostrando el estado del sistema en tiempo real y describiendo las acciones de mitigación realizadas sobre el sistema informático.

Esta estructura cíclica permite enriquecer las bases de conocimientos mejorando la capacidad de los sistemas informáticos a afrontar nuevas amenazas.

III. Conclusiones

La utilización de un software de gestión de parches como "IBM Smart Cloud" es una muy buena opción para empresas que manejan aplicaciones críticas en sistemas multiplataforma ya que por su nivel de granularidad esta herramienta proporciona una gran solución adaptándose a cada tipo de servidor que pueda estar corriendo en entorno virtual, aunque empresas que utilicen sistemas Windows el software de gestión System Center es una muy buena alternativa ya que brinda gestión de actualizaciones, consumo energético, gestión sobre servicios, revisión de procesos y rendimiento de sistemas operativos.

Los sistemas virtuales se han vuelto una interesante opción para los individuos malintencionados que desean realizar ataques cibernéticos desde estas plataformas a otras, en el caso de que un hacker logre acceder a una máquina virtual al realizar procedimientos sin mucho impacto en el procesamiento, consumo de memoria RAM, o ancho de banda puede permanecer desapercibido, con la ventaja que las máquinas virtuales poseen una vida corta, al finalizar determinada actividad el proceso de baja regular de la máquina virtual incluye además incluye el borrando los rastros de los ataques que hayan sido exitosos o no, por esta razón es fundamental mantener las actualizaciones del sistema operativo, aplicativos y antivirus vigentes, utilizando herramientas como "IBM SmartCloud Patch Management" para evitar cualquier tipo de explotación de vulnerabilidades.

Permanecer vigente en el mercado en muchas ocasiones requiere fuertes inversiones monetarias, que se ven compensadas con grandes ventajas, soluciones como la virtualización provee reducción de costos de implementación, aislamiento de los servicios, portabilidad, balanceo de carga y otras ventajas. En algunas situaciones se llegaría a pensar que la implementación de una máquina virtual es tan sencillo como oprimir un botón, lo cierto es que con cada máquina virtual corriendo en nuestro sistema el área de impacto aumenta, desplegar varias máquinas efectivamente es una labor muy sencilla pero hacerlo imprudentemente podría traer graves consecuencias para una organización, por ejemplo en el caso de que una imagen de una maquina posea una pobre configuración de seguridad el despliegue generaría la exposición de vulnerabilidades, "IBM SmartCloud Provisioning" posee una gran ventaja y es la generación de plantillas de configuración que se aplican en el momento de desplegar las máquinas virtuales, asegurando que cuenten con una configuración preestablecida basada en la vasta experiencia de IBM en múltiples sistemas operativos y aplicaciones, permitiendo entrar en operación con un nivel de riesgo aceptable

La Gestión de sistemas IDPS por parte de IBM es una estrategia muy razonable para la protección de los activos de la organización, ya que empresas con un objetivo de negocio diferente al de la tecnología, o empresas con talento humano inadecuado pueden simplificar y mejorar la seguridad de la información, subcontratando este tipo de servicios, aunque siempre existirá un riesgo residual al contratar un tercero para que administre la información, ya que en este tipo de situaciones se suele perder el control total de la información. Una gran ventaja de IBM frente a diferentes competidores es contar con una gran base de datos de millones de eventos a nivel mundial con la cual se pueden ejecutar correlaciones entre diferentes tipos de ataques, detectando con mayor precisión circunstancias peligrosas, y a la vez, contar con algoritmos de inteligencia artificial que detectan eventos totalmente nuevos que mejoran la probabilidad de mantener la información segura, esto hace de este servicio pieza clave para la continuidad del negocio.

Sistemas como "Endpoint Manager" son una valiosa herramienta ya que actualmente los mayores hoyos de seguridad se encuentran en los dispositivos portables, si una Tablet se pierde esta puede ser prácticamente formateada en el momento en que desde el software de gestión se genere la baja del dispositivo, los hackers ya no apuntan a los grandes sistemas de firewall porque saben que tener acceso desde un dispositivo portable es más fácil además burlar sus protecciones y extraer su información es más sencillo, con la implementación del Endpoint establecemos una capa de protección adicional que protege al sistema y/o brinda suficiente tiempo para tomar acciones preventivas o correctivas, servidores de autenticación AAA pueden verificar la salud de un dispositivo y determinar si puede o no tener acceso a la red de la compañía de esta forma se evita que dispositivo alterado gane acceso a la red y materialice diferentes tipos de riesgos de seguridad, además estos sistemas Endpoint están en constante comunicación con el centro de gestión permitiendo saber el usuario asignado al dispositivo, la ubicación geográfica del dispositivo, espacio de almacenamiento, estado del antivirus, nivel de batería, procesos ejecutándose, servicios corriendo, estado del cifrado de la información, tipos de conexiones realizadas cifradas y no cifradas.

El framework de gestión de parches de IBM muestra como es la forma de operación de la aplicación "Smart Cloud" o "Endpoint Manager", pero a nivel de procedimiento puede ser implementado en situaciones que incluso el uso de elementos informáticos no es esencial, un sistema informático que posee un alineamiento a la gestión y al modelo PHVA se puede alinear fácilmente a los objetivos de negocio de la organización, un ejemplo del poder de este Framework lo podemos representar de la siguiente manera, supongamos en el desarrollo de un sistema de control de inventario, en estos sistemas el procedimiento establece primero "Evaluar" lo que se tiene y hace falta, "Remediar" o solicitar productos faltantes o vencidos, "Fortalecer" el inventario en productos que se consumen con mayor velocidad o tienen una vida útil determina, o son difíciles de inventariar, y "Reportar" constantemente la situación del inventario para permitir al administrador del almacén tomar buenas decisiones, así como el modelo funciona bien para casos no relacionados a los

sistemas de cómputo su aproximación a estos lo hace muy poderoso si se analiza como una organización debe defenderse de delincuentes informáticos, por ejemplo, un hacker que desee atacar a una organización el proceso a realizar es recopilar información, escaneo de infraestructura, obtener acceso, mantener el acceso y eliminar rastros, al analizar las contramedidas propuestas por el Framework de IBM se puede observar que cubren y mitigan el riesgo en todos los aspectos de posible intrusión, por ejemplo al realizar el paso de evaluar se puede determinar el software que necesita actualizaciones, los procesos que están corriendo en el sistema, los puerto de la pila TCP/IP abiertos, los servicios activos esto evita abrir posibilidades para obtener acceso, en el paso de remediar corregiría situaciones anómalas evitando el mantenimiento del acceso por parte de un atacante y la recuperación de logs, en el paso de Reforzar se establecen reglas en firewall y acceso a los servicios evitando la recopilación de la información y escaneo de la infraestructura, y en el paso de Reporte se da a conocer el verdadero estado de la máquina determinando si se ha comprometido posibilitando acciones como aislamiento o supervisión además de informar las acciones tomadas para mitigar riesgos.

IV. Referencias

Documentación técnica:

[1] IBM, Simplify security management in the cloud, IBM Corporation Software Group, Route 100. Somers, NY 10589, Octubre 2012, Pag1.

[2] Nick Coleman, How does IBM deliver cloud security?, IBM Corporation Software Group, Route 100. Somers, NY 10589, Octubre 2012, Pag5.

[3] IBM, IBM SmartCloud Provisioning, IBM Corporation Software Group, Route 100. Somers, NY 10589, Enero 2013, Pag1.

[4] VMWARE, Understanding Full Virtualization, Paravirtualization, and Hardware Assist. VMWARE, Inc. 3401 Hillview Ave. Palo Alto CA 94304 USA, 2007, Pag4.

[5] Nick Coleman, How does IBM deliver cloud security?, IBM Corporation Software Group, Route 100. Somers, NY 10589, Octubre 2012, Pag2,.

[6] IBM, Intrusion detection and prevention system (IDPS) management, IBM Corporation Software Group, Route 100. Somers, NY 10589, Junio 2013, Pag2.