Artículo de Investigación

Gestión de Seguridad en Virtualización de Servidores

Security Management in Server Virtualization

Cordovilla, Felipe Arévalo; Arévalo Cordovilla, Braulio; Castillo Salvatierra, Luis; Cortez Lara, Alejandro

Felipe Arévalo Cordovilla
farevaloc@unemi.edu.ec
Universidad Estatal de Milagro, Ecuador
Braulio Arévalo Cordovilla
barevaloc@unemi.edu.ec
Universidad Estatal de Milagro, Ecuador
Luis Castillo Salvatierra
lcastillos1@unemi.edu.ec
Universidad Estatal de Milagro, Ecuador
Alejandro Cortez Lara
lcastillos1@unemi.edu.ec
Universidad Estatal de Milagro, Ecuador

Ecuadorian Science Journal
GDEON, Ecuador
ISSN-e: 2602-8077
Periodicidad: Semestral
vol. 5, núm. Esp.4, 2021
esj@gdeon.org

Recepción: 27 Noviembre 2021
Aprobación: 29 Diciembre 2021

URL: http://portal.amelica.org/ameli/jatsRepo/606/6062739014/index.html

DOI: https://doi.org/10.46480/esj.5.4.178

Como citar : Arévalo Cordovilla, F., Arévalo Cordovilla , B., Castillo Salvatierra, L., & Cortez Lara, A. (2021). Gestión de Seguridad en Virtualización de Servidores. Ecuadorian Science Journal, 5(4), 150-162. DOI: https://doi.org/10.46480/esj.5.4.178

Resumen: Este proyecto se centra en el campo de la seguridad en Servidores Virtuales en los entornos Cloud. En concreto, se estudia la seguridad a Infraestructura como Servicio (IaaS). Se estudia el caso específico de la minimización del riesgo relacionado a la seguridad al instalar máquinas virtuales en servidores físicos. Se analiza y describe como una máquina virtual vulnerable, puede comprometer a las otras máquinas virtuales vecinas e inclusive al servidor físico. En este estudio se propone un nuevo método para cuantificar el riesgo de seguridad para las máquinas virtuales. Los resultados arrojados por este método son tomados en cuenta para decidir la ubicación de un nuevo servidor virtual en un servidor físico con el fin de maximizar la seguridad. En este documento se proporciona una guía de buenas prácticas de seguridad centrada en la seguridad del servidor virtual.

Palabras clave: Cloud computing, IaaS, Seguridad informática, Virtualización.

Abstract: This project focuses on the field of Security in Virtual Servers in the Cloud environments. Specifically, the security at the IaaS is studied. The specific case related to minimization of risks when allocating new virtual machines into physical machines is studied. The case of how a vulnerable virtual machine that is allocated in a physical server can compromise the neighboring virtual machines and even the physical server is explained. In this study a new method for quantifying the security risk of virtual machines is proposed. This parameter helps in the decision-making task for choosing the physical server to install the new virtual server in order to maximize the security. A security good practice guide focusing on Virtual Server Security is provided in this document.

Keywords: Cloud computing, IaaS, Information Security, Security Threats, Virtualization.

Introducción

El mundo actual se caracteriza por la creciente tendencia al uso de las Tecnologías de la Información y las Comunicaciones (TICs), de los paquetes ofimáticos, de programas administrativos y contables, de programas educativos, entre otros, en todos los ámbitos de la sociedad. Estos recursos son utilizados tanto por organizaciones públicas, privadas, en el sector educativo, el sector industrial y empresarial, llegando a convertirse para todas estas instituciones en un factor importante de eficiencia, de competitividad y de asegurar la prestación de un mejor servicio o producto.

Uno de los problemas de mayor envergadura a los que las empresas u organizaciones deben enfrentarse para alcanzar estos objetivos, y principalmente las pequeñas y medianas, es el que se relacionan con la capacidad del crecimiento, del uso del hardware y software para cubrir sus necesidades operativas y les obliga a tener que abordar de forma continua aquellos temas que se relacionan con los costos, versatilidad, escalabilidad y funcionabilidad de estos componentes. Entre las opciones que existen para hacer frente la problemática descrita se encuentra la virtualización, es decir, crear máquinas virtuales que dupliquen el funcionamiento integro de la máquina real, "engañándola" para que funcione con toda su potencialidad como si se ejecutara una máquina normal cuando se está ejecutando es sobre una máquina virtual. La virtualización de los sistemas y herramientas se ha convertido en una de las soluciones más económica, provechosa y eficiente para dar respuesta a los problemas que se relacionan con el mejor aprovechamiento de estos recursos en la medida que les permite a las organizaciones darle un mejor uso y manejo de los recursos computacionales al mismo tiempo que logran disminuir el costo total asociado a los mismos.

En la actualidad la Computación en la Nube (Cloud Computing) se presenta como una nueva tendencia en TICs que se hace cada vez más popular, que representan cambios importantes en la forma en la que se almacenan y ejecutan aplicaciones de escritorio, aplicaciones y servicios Web, por medio de un a autoservicio bajo costos, moviendo la computación a la nube.

La computación en la nube como una nueva forma de operar proporciona una infraestructura eventualmente ilimitada para almacenar y ejecutar datos y programas de clientes en donde los clientes no necesitan tener su propia infraestructura, sino sólo acceso vía Web, entre los principales modelos de servicio que ofrece la computación en la nube según Lisdorf (2021) se encuentran:

1. Software como servicio (SaaS), es un modelo donde todo lo gestiona el vendedor. No puede programar nada usted mismo, solo lo configura y usa a través de un navegador web. Algunos ejemplos comunes son los servicios de Google como Documentos, Calendario y Hojas de cálculo o Office 365 de Microsoft. Estos brindan al usuario solo opciones limitadas para configurar el software. Muchas aplicaciones empresariales entran en esta categoría, como Oracle HCM, ServiceNow, Zendesk y más.
2. Plataforma como servicio (PaaS), es un poco menos sencillo y los ejemplos son más heterogéneos. Este modelo de servicio se refiere a plataformas que el consumidor puede utilizar para programar aplicaciones. Es posible escribir código y configurar el servicio, pero el proveedor administra la infraestructura subyacente.
3. Infraestructura como servicio (IaaS), es la forma más básica donde se proporcionan recursos informáticos básicos y el consumidor instala y administra el software necesario. Este modelo ofrece el mayor control, pero también requiere más trabajo.

Pero estas nuevas tecnologías y sus ventajas no se encuentran exenta de problemas o riesgos, vale señalar que la principales desventajas que presentan es la que se relaciona con la seguridad de estos entornos, esta desventaja de seguridad se materializa en un aumento "casi exponencial" de la superficie de ataque del entorno virtualizado y en la computación en la nube se manifiesta en la protección de la seguridad y privacidad de datos y programas y de la falta de un control directo por parte del usuario.

Mientras que a nivel de la nube, además de los nombrados apa-recen otros problemas como pueden ser; vulnerabilidades en el proveedor de la computación en la nube (cloud computing), ataques a nivel de Máquina Virtual (MV) aprovechándose de vulnerabilidades en el hipervisor o tecnología MV utilizada por los proveedores de nubes lo que es muy común en arquitecturas de multi-arrendamiento, Phishing/Scams en proveedores de la computación en la nube (cloud computing), dificultad para realizar análisis forense en la nube, dificultad para la autenticación y autorización, expansión de la superficie de ataque de red, entre otros.

La aparición de estas fisuras de seguridad en los entornos virtualizados a nivel organizacional se debe a que el flujo de información entre máquinas virtuales no atraviesa ningún dispositivo de seguridad perimetral de los existentes, originando los denominados "Puntos Ciegos" para la seguridad.

El problema en IaaS Clouds

Uno de los actuales desafíos en la implementación de IaaS es determinar la ubicación de la máquina virtual, por ejemplo, asignar cada máquina virtual a un equipo físico en la infraestructura del proveedor de IaaS Cloud.

Algunas estrategias han sido implantadas para IaaS, estas estrategias son basadas en varios criterios. Un ejemplo de esta estrategia es "Scatter-Gather live migration". En general, las métricas de rendimiento que se utilizan para medir la eficacia de la migración de una máquina virtual son el tiempo total de migración y el tiempo de inactividad. Según Deshpande et al. (2018) propuso un nuevo parámetro - tiempo de desalojo y desarrolló un nuevo mecanismo de migración de VM - migración de VM Scatter-Gather para reducir el tiempo de desalojo. El tiempo de desalojo se define como el tiempo necesario para desalojar por completo el estado de una o más máquinas virtuales que se migran del host de origen. Las siguientes situaciones exigen el desalojo rápido de una máquina virtual: emplee mecanismos oportunistas de ahorro de energía desactivando el exceso de capacidad del servidor, eliminación rápida del punto de acceso para garantizar el rendimiento, desalojando inmediatamente las máquinas virtuales de menor prioridad para dar cabida a otras de mayor prioridad otros, realizar mantenimiento de emergencia o para manejar fallas inminentes. Por otra parte, la técnica "energy-aware VM placement" pretende optimizar la implantación y ubicación las máquinas virtuales con el fin de minimizar el consumo energético en el cloud(Fu et al., 2018).

Existen pocos esfuerzos que incorporan el manejo de riesgos y seguridad en la implantación de máquinas virtuales. Los riesgos de seguridad es uno de los factores más importantes a considerar que influencian el desarrollo y la aceptación de IaaS clouds en aplicaciones prácticas, pero lamentablemente en realidad prevalecen las vulnerabilidades más comunes en máquinas virtuales públicas que los proveedores proveen(Rakotondravony et al., 2017).

Bhagat et al. (2020), los autores mostraron que, las principales fuentes de vulnerabilidades en las máquinas virtuales son los sistemas operativos, la mala configuración y las aplicaciones instaladas en ellas. Por ejemplo, puertos abiertos no utilizados, uso de una cuenta y contraseña predeterminadas, autenticación y autorización débiles (incluida la autenticación de múltiples factores faltante o ineficaz, control de acceso débil de los recursos, recuperación de credenciales débil o ineficaz y proceso de olvido de contraseña), habilitar o instalar funciones innecesarias. La mala configuración es uno de los factores principales detrás de los ataques a IaaS. Un permiso mal configurado conduce a la mayoría de los ataques de violación de datos en la aplicación web en la nube

Según Bugiel S et al. (2011) al escanear un cierto número de imágenes de máquinas virtuales, se encontró que las imágenes poseían información privada como claves, llaves y otras credenciales. Esta información delicada que por negligencia existe en varias imágenes de máquinas virtuales, puede encadenar un considerable número de ataques hacia los otros servidores virtuales que se encuentran alojados en un IaaS Cloud.

FIGURA 1.
Ejemplo de grafo de ataque a máquinas virtuales
Elaboración propia

La Figura 1 muestra como cuando se introduce una nueva imagen de una máquina virtual en un servidor físico, existe un alto riesgo de vulnerabilidad hacia las imágenes de máquinas virtuales ya instaladas en dicho servidor físico.

Esto se debe al hecho de la relación 1 a n entre el servidor físico y las máquinas virtuales, lo cual hace que las vulnerabilidades se propaguen rápidamente en la infraestructura del IaaS. Inclusive el servidor físico que contiene todas las imágenes de las máquinas virtuales podría ser tomado por el atacante si la máquina virtual del hipervisor (Servidor virtual 1) se encuentra comprometida con las mismas vulnerabilidades que las otras máquinas virtuales.

Por ejemplo, uno de los ataques más comunes en una infraestructura IaaS son los ataques de canal lateral a través del servidor virtual 1 por medio de la co-ubicación de los servidores virtuales. Los atacantes pueden mapear la ubicación de las máquinas virtuales internas en el cloud y realizar ataques de canal lateral instalando servidores virtuales maliciosos en la máquina física de la víctima. En resumen, con el nuevo modelo de cloud público, es fácil para los atacantes lanzar ataques a través de vulnerabilidades predominantes.

Obviamente estos ataques son basados en la ubicación de los servidores virtuales y su éxito netamente depende de las estrategias de ubicación del cloud. Por lo tanto, la ubicación de un servidor virtual puede causar un impacto en el las condiciones de seguridad del cloud. Para minimizar los riesgos de seguridad en el cloud y poder aliviar la seguridad de servicios los clientes es necesario desarrollar una estrategia segura de ubicación de servidores virtuales en el cloud donde las máquinas virtuales con alto riesgo pueden ser separadas de las máquinas virtuales de bajo riesgo. De igual manera la probabilidad de ubicar o instalar una máquina virtual vulnerable en un servidor físico con un alto nivel de seguridad debe ser minimizado.

Evaluación de la seguridad de servidores virtuales en IaaS Clouds

La evaluación de seguridad consiste en evaluar los riesgos de los servidores tanto físicos como virtuales en el cloud.

Existe una base de datos de vulnerabilidades publica y periódicamente actualizada por una entidad gubernamental de los Estados Unidos de Norte América(National Vulnerability Database, 2021), esta base de datos se llama “US National Vulnerability Database (NVD)”. En esta base de datos las vulnerabilidades son marcadas o clasificadas dependiendo de su Sistema de puntuación de vulnerabilidad común (Common Vulnerability Scoring System (CVSS))(Common Vulnerability Scoring System SIG, 2021).

Basados en estos datos se puede calcular la probabilidad de riesgo de cada servidor virtual explorando las relaciones de dependencia entre las máquinas virtuales en el cloud. De igual manera se puede inferir en una calificación o clasificación de cada servidor físico dependiendo en el nivel de riesgo de seguridad de las máquinas virtuales alojadas en este.

Materiales y Métodos

El presente estudio se fundamentará en el paradigma positivista, el cual según Meza citado por Hurtado y Toro (2007), ". . . concibe la realidad como única y, la misma, puede ser fragmentada para su análisis y las partes pueden ser manipuladas independientemente" (p.58), lo que permite abordar un problema que en realidades solamente de un todo mucho mayor. El mismo está enmarcado en una investigación de campo de carácter descriptivo, definido por Hernández-Sampieri Roberto & Mendoza Torres Christian (2018) como:

> ". . . las propiedades, características y perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, miden o recolectan datos y reportan información sobre diversos conceptos, variables, aspectos, dimensiones o componentes del fenómeno o problema a investigar. En un estudio descriptivo el investigador selecciona una serie de cuestiones (que, recordemos, denominamos variables) y después recaba información sobre cada una de ellas, para así representar lo que se investiga (describirlo o caracterizarlo)." (p.108)

Las características de las investigaciones de campo es que se van a caracterizar porque los problemas que se estudian por medio de este tipo de investigación es un problema que se evidencia en la realidad. Es por ello que el presente estudio se enmarca dentro de este tipo de investigación debido a que, aunque la tecnología de la virtualización avanza a pasos agigantados no lo ha hecho de igual forma la tecnología, la normativa y los procedimientos administrativos y de gestión colaterales necesario para ofrecerle la adecuada seguridad al producto de esta tecnología.

En este sentido lo que se busca es la de lograr una unificación de los diferentes criterios que existen en el ámbito informático sobre la protección de los servidores, a los escritorios, a las redes o a los centros de información que han sido virtualizados para de esta forma realizar una selección de los más pertinentes a ser reunidos en un manual que sirva como un paso en pro de la búsqueda de solución de problemas dentro de ese contexto.

En función a los anterior es que la presente investigación se circunscribe en esa modalidad, debido a que el propósito fundamental es el de Presenta una propuesta de un Manual de Gestión de seguridad para entornos virtualizados que reduzca los riesgos y amenazas por medio de la aplicación de un conjunto de políticas de seguridad informática y administrativas que ayuden a una gestión de estos entornos.

Para la realización de este trabajo se ha seguido la estrategia de realizar la búsqueda, recopilación, análisis, selección del material informacional disponible en la internet u otro medio disponible para posteriormente utilizarlo en la preparación del Manual como una forma de presentar una guía de seguridad que sea homogénea a los diferentes entornos virtualizados y de esta forma superar la actual limitante de incompatibilidad que existen entra las diferentes políticas de seguridad aplicables a los entornos virtualizados.

La principal contribución de este documento es la propuesta de un nuevo método para la cuantificación del riesgo al ubicar nuevas máquinas virtuales. Las fórmulas descritas en el desarrollo son netamente propuestas por el autor de este trabajo. El método de reubicación de máquinas virtuales en un servidor físico se basa en un algoritmo pragmático de complejidad baja.

Para reforzar la seguridad en los servidores virtuales se adjunta un Manual de Gestión de seguridad para entornos virtualizados con el objetivo de exponer en el mismo un conjunto de medidas y políticas que sirvan de guía y ayuda para reducir los riesgos y amenazas a las cuales se encuentran sometidos estos ambientes o entornos.

Esta propuesta tiene su iniciativa en el hecho de que los sistemas virtualizados, sin importar cuál sea su tamaño u orientación de virtualización crecen cada día pero a la par de este crecimiento cada día es también mayor el número de atacantes más organizados y tecnificados que quieren aprovecharse de las debilidades presentes en los entornos virtualizados, y si a este hecho se suma las fallas de seguridad provenientes del interior mismo de la organización hacen necesario enfrentar y subsanar estas debilidades.

Aunque la propuesta de un Manual de Gestión de seguridad para entornos virtualizados está dirigida principalmente hacia estos entornos también abordan las amenazas informáticas que afectan por igual tanto

a los sistemas basados en hardware como a los entornos virtuales, y aunque cada entorno posee una serie de condiciones que le son propias e inherentes, pero al momento de implementar políticas y medidas de seguridad no son excluyentes entre ellas, sino más bien complementarias.

Resultados y Discusión

La clasificación de los CVSS es la métrica principal para poder ponderar el nivel de peligro de la vulnerabilidad. Esta clasificación se encuentra en una escala del 1 al 10 la cual corresponde al nivel de severidad nula, bajo, medio, alto, y crítica como se muestra en la tabla 1. Los detalles se encuentran en (National Vulnerability Database, 2021).

TABLA 1
Grados de vulnerabilidad otorgados por la NVD

Tabla 1. Grados de vulnerabilidad otorgados por la NVD

Gravedad	Ponderación
Nula	0.0
Baja	entre 0.1 y 3.9
Media	entre 4.0 y 6.9
Alta	entre 7.0 y 8.9
Crítica	entre 9.0 y 10.0

Fuente: NVD. US National Vulnerability Database

NVD. US National Vulnerability Database

1. En este proceso primeramente se verifica la NVD para recolectar eventuales vulnerabilidades tanto del Sistema Operativo como del Software que presta servicios específicos (ej. File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) en los servidores virtuales.
2. Luego se procede a realizar un escaneo de vulnerabilidades con herramientas como Nessus y Qualys (permiten la detección de vulnerabilidades actuales en sistemas de información).
3. Es muy probable que existan varias vulnerabilidades en un servidor virtual virgen, por lo que hay que asignar una ponderación a cada vulnerabilidad encontrada en cada servidor virtual.
4. Se escoge la vulnerabilidad más crítica encontrada (Clasificación basada en el CVSS) de cada servidor virtual. Se asume que el nivel de vulnerabilidad no es más alto que la vulnerabilidad más débil de este servidor virtual.
5. Una vez que se cuantificado el nivel de vulnerabilidad de cada servidor virtual, se procede a mapear la vulnerabilidad cuantificada a la probabilidad de que las otras máquinas virtuales que se encuentran instaladas en el mismo servidor o infraestructura puedan verse comprometidas con dicha vulnerabilidad. En este mapeo se usa información topológica básica como la dirección Internet Protocol (IP) y de red, números de puertos, etc, generadas por herramientas de red como netstat.

Una vez obtenida todas las relaciones de dependencia, se puede construir un grafo de dependencia de máquinas virtuales como se muestra en la Figura 2.

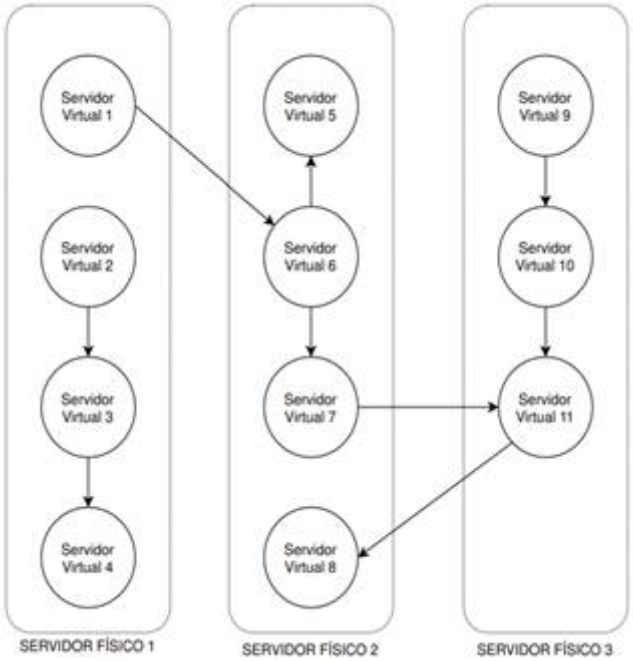

FIGURA 2.
Mapeo de servidores virtuales
Elaboración propia

Para mapear las vulnerabilidades cuantificadas que podrían comprometer o afectar otras máquinas virtuales según las relaciones de dependencia se calcula un índice de vulnerabilidad de todas las MVs instaladas en el servidor físico.

Asumir un servidor virtual (máquina virtual) como MV_a cuyo índice de vulnerabilidad es ${}^{IV}MV_a$, el índice de vulnerabilidad de las otras máquinas virtuales conectadas a esta es:

$\{{}^{IV}MV1, {}^{IV}MV2, {}^{IV}MV3, \ldots, {}^{IV}MVn\}$

El índice de vulnerabilidad del servidor físico IVSF es calculado con la Ecuación 1.

$$IV_{SF} = \frac{\sum_{i=1}^{n} IV_{MV_i}}{n} \quad [1]$$

La ecuación (1) da como resultado un índice entre cero y diez. Este índice es muestra el riesgo seguridad del servidor físico tomando en cuenta cada índice de seguridad de que cada máquina virtual que esta aloja. El índice de riesgo es el mismo que el descrito en la tabla 1.

Para calcular el índice de compatibilidad IC entre el servidor físico SF y la máquina virtual MVa a ser ubicada en ese servidor se usa la ecuación 2.

$$IC = \left|\left(IV_{SF} - IV_{MV_a}\right) \times 0.1\right| \quad [2]$$

Mientras el valor de IC tienda a cero más compatible es la máquina con el servidor físico, por lo contrario, mientras el valor de IC tiende a 1 la máquina virtual a ser instalada no es compatible con el servidor físico.

Ejemplo (caso 1):

Según la NVD, la máquina virtual nueva a ser ubicada en un servidor físico posee un índice de vulnerabilidad IV =9. El servidor físico posee 5 máquinas virtuales instaladas (MV_1, MV_2, MV_3, MV_4 y MV_5) con índices de vulnerabilidad IV_{MVi}, de (9, 10, 7, 5 y 8) respectivamente.

Según la ecuación (1), el índice de vulnerabilidad del servidor es:

$IV_{SF} = 7,8$.

Aplicando la ecuación (2), el índice de compatibilidad entre la máquina virtual y las otras máquinas virtuales instaladas en el servidor físico es:

IC = 0,12.

Esto significa que todas las máquinas virtuales del servidor físico poseen un índice de vulnerabilidad muy aproximado al de la máquina virtual a instalarse en el servidor físico.

Ejemplo (caso 2):

Según la NVD, la máquina virtual nueva a ser ubicada en un servidor físico posee un índice de vulnerabilidad IV =1. El servidor físico posee 5 máquinas virtuales instaladas (MV_1, MV_2, MV_3, MV_4 y MV_5) con índices de vulnerabilidad IV_{MVi}, de (9, 10, 7, 5 y 8) respectivamente.

Según la ecuación (1), el índice de vulnerabilidad del servidor es:

$IV_{SF} = 7,8$.

Aplicando la ecuación (2), el índice de compatibilidad entre la máquina virtual y las otras máquinas virtuales instaladas en el servidor físico es:

IC = 0,68.

Esto significa que todas las máquinas virtuales del servidor físico poseen un índice de vulnerabilidad muy alejado al de la máquina virtual a instalarse en el servidor físico, lo cual significa que existe un gran riesgo de contagio de vulnerabilidad si comparten servidor físico.

Método de asignación de nuevas máquinas virtuales en una máquina física

El objetivo de este método es minimizar la probabilidad de vulnerabilidades tanto en un servidor virtual como en el servidor físico que alberga las máquinas virtuales. Se ha estudiado el impacto de la vulnerabilidad y se mencionó que un ataque exitoso depende de la estrategia de ubicación de las máquinas virtuales en el cloud.

Este método propuesto se enfoca en minimizar el riesgo tanto para el servidor virtual como para el servidor físico. Para una máquina virtual cuya probabilidad de riesgo es baja, no debería ser ubicada en una máquina física cuyo índice de supervivencia es bajo. Esto aumentaría la probabilidad de riesgo de una máquina virtual.

Por otra parte, en el caso de un servidor físico con alta probabilidad de supervivencia, no debería alojar máquinas virtuales con alta probabilidad de riesgo, pues esto causaría un considerable impacto en el nivel de supervivencia de la máquina física. Por lo tanto, un método inteligente debe minimizar el riesgo y maximizar la supervivencia del servidor físico simultáneamente. Por ejemplo, es lógico y razonable que una máquina virtual con baja probabilidad de riesgo sea instalada en un servidor físico con alta probabilidad de supervivencia.

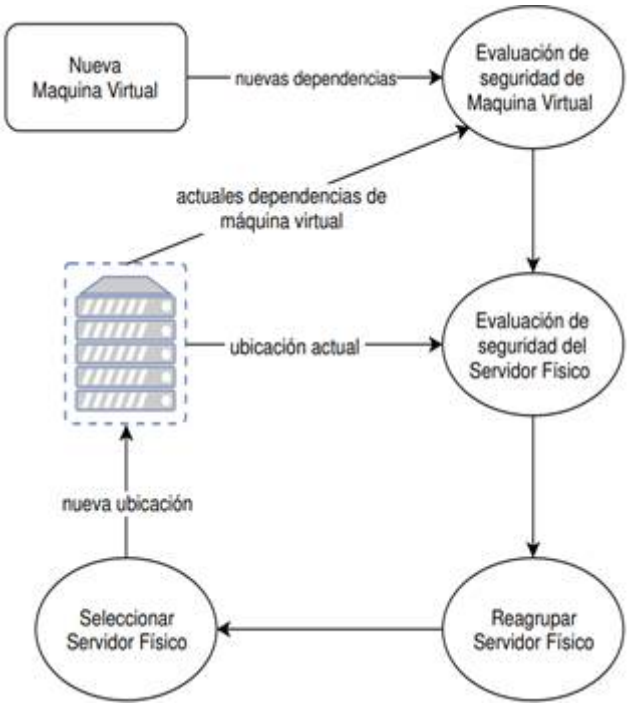

FIGURA 3
Esquema general de ubicación de máquinas virtuales
Elaboración propia

La Figura 3 representa el esquema propuesto para la asignación de máquinas virtuales a servidores físicos. Cuando una nueva máquina virtual necesita ser instalada se debe actualizar el índice de riesgo de todas las máquinas virtuales instaladas según lo muestra la ecuación 1 basado en las relaciones de dependencia introducidas por la nueva máquina virtual.

El siguiente paso es reagrupar las máquinas virtuales en diferentes servidores físicos basadas en su índice de riesgo.

A continuación, se describe este proceso en el Algoritmo 1.

ALGORITMO 1
Ubicación de servidores virtuales (mv, SF, MV)

Algoritmo 1 Ubicación de servidores virtuales (mv, SF, MV)
1. Datos de entrada: mv: nueva máquina virtual a ser ubicada SF: Lista de servidores físicos disponibles en el cloud MV: Lista de máquinas virtuales presentes en cada servidor físico
2. repeat (para cada sfi ∈ SF)
3. repeat (para cada mvj ∈ sfi)
4. Calcular IC según ecuación (2)
5. Agrupar o reagrupar la mvj en un sfi dependiendo de su IC
6. until no existan más máquinas virtuales
7. until no existan más servidores físicos

El mecanismo presentado previamente, a mi criterio debe ser complementado con un conjunto de buenas prácticas a ser implementadas relacionadas al IaaS. En esta sección se describe las políticas mínimas a seguir, lo cual se describe en las normas de seguridad de los entornos virtualizados y cloud computing.

Manual de Gestión de seguridad para entornos virtualizados

Normas de seguridad de los entornos virtualizados

1. Debe existir una política de autentificación robusta de usuario para restringir el acceso al (los) huésped(es), solamente a aquellos usuarios autorizados.
2. Se debe implementar la Seguridad del Server HOST o del Storage a través de la aplicación de permisos de acceso a las máquinas virtuales.
3. Se debe implementar una normativa de encriptación de datos para evitar que la información que se encuentra en la máquina virtual o que fluye por medio de la red pública puedan ser leídos por personas no autorizadas.
4. Las llaves de llaves de encriptación para el cliente y el servidor se deben generar y renovar de forma periódica según patrones establecidos.
5. Se deben mantener actualizados los soportes para los protocolos más comunes o usuales utilizados en las redes públicas.
6. Para asegurar que la interconexión entre redes virtuales se debe implementar Protocolo de Túneles (PPTP, LTTP, IPSEC); encapsulación y encriptación de las tramas emulando un enlace punto a punto privado seguro sobre la infraestructura pública usada; de las conexiones VPN, con la finalidad de cumplir las necesidades de seguridad de los datos transmitidos. Se pueden combinar los protocolos LTTP, IPSEC.
7. Se deben siempre herramientas de seguridad que hayan sido diseñadas para trabajar con los aspectos dinámicos del entorno virtual y puedan detectar los problemas automáticamente y proteger las máquinas virtuales.
8. Deshabilite las Funciones Innecesarias o Superfluas
9. Se deben utilizarse los mecanismos de seguridad específicos de las máquinas virtuales que se encuentran incorporados en las APIs del hipervisor para proporcionar una monitorización granular del tráfico que pasa por las backplanes de estas máquinas.
10. Los sistemas operativos virtualizados deben incluir firewall (entrante/saliente), sistema de prevención de intrusiones en host (HIPS), sistema de prevención de intrusiones en red (NIPS), protección de aplicaciones web, antivirus, monitorización de integridad de archivos, monitorización de logs, etc.
11. Se deben diseñar una política de eliminación de las copias de seguridad y sistema de respaldo cuando elimine y borre las imágenes de la máquina virtual.
12. Se deben diseñar una política para el continuo mantenimiento y actualización de las imágenes de máquinas virtuales en reposo y de protección de las nuevas VM hasta que sean parchear.
13. Las máquinas virtuales no utilizadas deben ser cifradas mientras no estén en uso.
14. Se debe definir claramente los roles y acceso de los usuarios del sistema.
15. Se debe separar físicamente, al menos, las redes de almacenamiento, gestión y máquinas virtuales.
16. Se debe utilizar los programas Monitores de máquinas virtuales (VMMs) que tengan acceso a todos los estados de una VM, incluyendo el estado del CPU, de la memoria y de los dispositivos y con capacidades de inspección que propicien checkpoints, rollbacks y replays.

17. Se debe aplicar una política de aislamiento de máquinas virtuales, por medio de la instalación las VM en particiones o volúmenes diferentes que cuente con un mecanismo de reporte que ofrezca pruebas del aislamiento y active alertas si hay una violación del aislamiento.
18. Las VM's deben tener asignados recursos fijos para su funcionamiento.
19. Implementar mecanismos para lograr un control de detección del tráfico por medio de la generación de reportes tales como: los horarios de accesos al entorno virtual, el registro de tráfico entre maquina virtuales, el flujo de datos valorizado entre VM, cuáles son las maquinas conectadas y los accesos externos, reporte de host activos y tiempo de actividad, análisis de protocolos y rendimiento de comunicación y de alertas por detección de tráfico malicioso y accesos no permitidos.
20. Establecer controles de seguridad en cada capa dentro de la arquitectura virtual, incluidos los controles de la red de la organización. Las capas virtuales primarias que proteger son la del hipervisor, los sistemas operativos hospedados, la red virtual entre máquinas virtuales, la red física, el sistema de gestión de la virtualización y el almacenamiento físico de las imágenes virtuales.
21. Utilizar la consola de gestión de Trend Micro a fin de supervisar y notificar de cambios importantes en los sistemas críticos.
22. Utilizar los switches virtuales para asegurar la red virtual contra ataques potenciales del tipo man-in-the-middle.
23. Implementar un aparato virtual con acceso a comunicación con sitios externos que le permitan descargar información actualizada sobre amenazas para que desempeñe todas las funciones de una solución de seguridad como si fuera una sola máquina virtual que se encargara de supervisar a todas las máquinas virtuales por medio hipervisor.
24. Maximizar el aislamiento de las instancias que se ejecutan en la misma máquina.

Normas de seguridad a nivel de Cloud Computing

1. Se debe firmar un contrato de servicio que como mínimo contemple que el proveedor de servicios firme un acuerdo de confidencialidad y no divulgación de datos a los que pudiera tener acceso durante la provisión del servicio. DE igual forma se deben contemplar en el mismo: Retención de datos, Service Level Agreement, Responsabilidades, Jurisdicción, Privacidad, Leyes sobre Seguridad, Pedidos de información y Cumplimiento de regulaciones y auditorias
2. Se debe constatar que el proveedor cuente con políticas muy estrictas para la destrucción de información que pudiera encontrarse en hardware que se retira de servicio activo.
3. Implementar el uso de servidor proxy inverso (reverse proxy), que proporcione un punto de acceso único a la red interna y el mismo debe estar habilitado como componente de autenticación y de control de acceso a las aplicaciones WEB.
4. Hacer uso de certificados digitales emitidos por autoridades de confianza, que permitan a las aplicaciones cliente verificar que realmente está conectado con el proveedor de servicio correcto
5. Utilizar el Protocolo ligero de acceso a directorios (LDAP, Lightweight Directory Access Protocol), los más usados son; Oracle directory server, IBM Tivoli Directory Server y OpenLDAP.
6. Utilizar un dispositivo de seguridad IPS (Intrusion Prevention System) para prevenir posibles intrusiones a partir de la identificación y bloqueo de patrones específicos de ataque en su flujo por la red, más utilizados: Snort, CISCO Firepower, Checkpoint y Suricata.
7. Implementar mecanismos de Intrusion Detection System (IDS) integrados al cortafuego que funcionen en tiempo real para detectar actividades inapropiadas, incorrectas o anómalas en la red de una organización
8. El uso de Secure Sockets Layer (SSL) y Transport Layer Security (TLS) para el cifrado de la información.

9. Utilizar herramientas de escaneo de vulnerabilidades, los más usadas son; Nessus, Nmap, OpenVAS.
10. Solicitarle al proveedor que nuestras máquinas virtuales sean ubicadas en una zona desmilitarizada (DMZ), y si es necesario requerir equipos de red independientes como Switches dedicados por los cuales sólo fluya el tráfico destinado solamente a las máquinas virtuales de la organización.
11. Solicitar al prestador de servicios que utilice VLAN Tagging o Truking para las máquinas virtuales a fin de asegurar que todos los paquetes que entran o salen de las máquinas virtuales de la organización tengan un ID de VLAN que sólo las interfaces de red en la misma VLAN reciban y procesen esos paquetes.
12. Es recomendable, Si se puede, alquilar el servidor físico completo para el uso exclusivo de las máquinas virtuales de la organización evitando tener que compartirlo con otros inquilinos.
13. Programar la realización de copias de seguridad a un tiempo definido.
14. Elija almacenamiento con dispersión de los datos cuando esté disponible.
15. Utilice el ciclo de vida de seguridad de los datos para identificar riesgos de seguridad y determinar los controles más adecuados.
16. Monitorice las bases de datos clave internas y los repositorios de archivos con DAM y FAM para identificar grandes migraciones de datos, que podrían indicar que se están migrando datos al Cloud.
17. Monitorice el acceso de los empleados a Internet con filtrado de URL y/o herramientas DLP para identificar datos delicados que se estén migrando al Cloud

Conclusiones

La seguridad relacionada a los servidores virtuales es altamente general, por lo que este estudio se enfoca netamente en la seguridad de IaaS en los servidores virtuales.

Aunque las tecnologías de virtualización han adquirido una velocidad impresionante de adopción, y que al momento de realizar un balance entre los beneficios de la virtualización versus sus retos y los riesgos que se deben asumir cuando se decide optar por la virtualización, virtualizar gana el reto. No significa que aquellas personas u organizaciones que se decidan a implementar esta tecnología deban darse por satisfechas por el simple hecho de haber ganado ventajas en su sistema informático.

Toda persona u organización que se decida por la virtualización debe tener bien claro que la tecnología de seguridad tradicional estructurada para los sistemas de hardware no tiene el mismo funcionamiento en los entornos virtuales. Por otro lado, todo entorno virtualizado a la larga es un sistema híbrido en algún sentido, en toda organización existe una mezcla de los sistemas virtuales y sistemas físicos y los sistemas virtuales dependen de los sistemas físicos para poder existir y poder realizar su función. Lo anterior indica que para querer implementar medidas de seguridad de lo sistema virtualizados se debe dar inicio por ofrecerle seguridad en primera instancia al entorno físico para continuar con el del entorno virtualizado, pero este proceso no debe verse como partes separadas por el contrario debe verse como un todo holísticos.

Para evitar la aparición de los agujeros normativos de seguridad, cuando estos se relacionan con los entornos virtualizados lo recomendable es que las organizaciones que utilizan estas tecnologías se mantengan informadas y actualizadas sobre las disposiciones que emanan de los organismos especializados en normalizar y estandarizar la gestión de la seguridad a nivel mundial. Organismos como los CERTs o CSIRTs, NVD o el FIRST deben ser usados como una fuente de información actualizada para poder obtener datos reales sobre las nuevas vulnerabilidades encontradas recientemente.

Los métodos de seguridad al instalar una máquina virtual deben tomar en cuenta tanto el servidor virtual como el servidor físico. Por su parte el proveedor debería entregar al cliente, un manual de actualización del

sistema operativo y servicios alojados en la máquina virtual. Por su parte el cliente debe actualizar su sistema operativo de manera periódica.

Trabajo Futuro

Enfocarse en soluciones de aislamientos de máquinas virtuales para evitar ataques en cadena en el mismo servidor físico. Así mismo usar técnicas de deep learning para contrarrestar la polaridad de los promedios.

Referencias Bibliográficas

Bhagat, S. P., Patil, V. S., & Meshram, B. B. (2020). Security Issues Due to Vulnerabilities in the Virtual Machine of Cloud Computing. Advances in Intelligent Systems and Computing, 1034, 625–634. https://doi.org/10.1007/978-981-15-1084-7_60

Bugiel S, Nurnberge S, Poppelmann T, Sadeghi A, & Schneider T. (2011). AmazonIA: when elasticity snaps back. 726.

Common Vulnerability Scoring System SIG. (2021). https://www.first.org/cvss/

Deshpande, U., Chan, D., Chan, S., Gopalan, K., & Bila, N. (2018). Scatter-Gather Live Migration of Virtual Machines. IEEE Transactions on Cloud Computing, 6(1), 196–208. https://doi.org/10.1109/TCC.2015.2481424

Fu, X., Zhao, Q., Wang, J., Zhang, L., & Qiao, L. (2018). Energy-Aware VM Initial Placement Strategy Based on BPSO in Cloud Computing. Scientific Programming, 2018. https://doi.org/10.1155/2018/9471356

Hernández-Sampieri Roberto, & Mendoza Torres Christian. (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.

Lisdorf, A. (2021). Cloud Computing Basics. In Cloud Computing Basics. Apress. https://doi.org/10.1007/978-1-4842-6921-3

National Vulnerability Database. (2021). https://nvd.nist.gov/

Rakotondravony, N., Taubmann, B., Mandarawi, W., Weishäupl, E., Xu, P., Kolosnjaji, B., Protsenko, M., de Meer, H., & Reiser, H. P. (2017). Classifying malware attacks in IaaS cloud environments. Journal of Cloud Computing, 6(1). https://doi.org/10.1186/s13677-017-0098-8