Kaspersky
Hybrid Cloud
Security

Tiene problemas con la seguridad de las instancias en las nubes públicas.

2019

kaspersky

Obtenga más información en kaspersky.com/hybrid

Tiene problemas con la seguridad de las instancias en las

Introducción

El uso público de la nube está creciendo porque proporciona muchos beneficios, incluyendo escalabilidad instantánea, automatización, capacidad de configuración y flexibilidad. Todas aquellas personas que se dedican a la implementación de la administración pública en la nube, tanto los equipos de Seguridad de la información como los que no están involucrados con esta disciplina (por ejemplo, Dev Ops o Web Dev) necesitan garantizar que la seguridad de los activos de la empresa se considere el pilar fundamental de la planificación.

Este informe está diseñado para proporcionarle a los especialistas de InfoSec toda la información y pruebas necesarias para garantizar que las cargas de trabajo en la nube funcionen de manera segura, por ejemplo, que la seguridad del sistema operativo la cual ejecuta la carga de trabajo se considere como un aspecto fundamental en los escenarios de implementación de la nube. Después de todo es su problema, ya que si se vulnera la seguridad en la nube, técnicamente la persona que sea culpable de que esto ocurra siempre tendrá que asumir las consecuencias.

Nuestro objetivo es contrarrestar la percepción errónea de que ciertas cosas como la explotación de vulnerabilidades en el software (evasión del inicio de sesión, ejecución de códigos a distancia, etc), las actualizaciones que contaminan los depósitos, la explotación de las conexiones de red (por ejemplo, el secuestro del DNS), y el compromiso de la información de la cuenta solamente ocurren en entornos físicos o virtuales, pero no en las nubes públicas. O que, en entornos de nubes públicas, el daño causado a su información u organización como consecuencia de un incidente en la seguridad, de alguna manera ya no es su problema.

Además, en este documento se hace referencia a algunos riesgos empresariales específicos que implican las nubes públicas, incluido el robo de recursos de la nube. La escalabilidad instantánea en la nube significa que los cibercriminales que se apoderan de sus controles en la nube pueden aumentar y utilizar volúmenes casi infinitos de la capacidad informática en su nombre y a costa suya. De cualquier modo, proteger completamente la infraestructura de su nube pública es una elección de inversión inteligente.

Vulnerabilidades en las nubes públicas

Además de los problemas de seguridad más temidos (y con justa razón) a los que se enfrenta en las nubes públicas, como poner el peligro la cuenta y errores en la configuración, existen vectores de amenazas dirigidos a las instancias, que utilizan las vulnerabilidades en los servicios con exposición a Internet, servicios como RDP y SSH.

El RDP está activo de forma predeterminada en las instancias de Amazon, y su diseño no es compatible con la autenticación de 2 factores. El RDP se convirtió en el objetivo de muchos y diferentes tipos de ataques. Algunos ataques utilizan solamente los inicios de sesión más frecuentes conforme forzan la autenticación de la contraseña, mientras que otros atacan los inicios de sesión mediante las contraseñas que se utilizan con más frecuencia. Algunos atacantes limitan y hacen aleatorio el número de intentos para el inicio de sesión, con un tiempo de espera entre series de intentos, para evitar la detección automática. Otro método de ataque es forzar la autenticación de la contraseña para el servicio de inicio de sesión SSM del usuario, el cual algunas veces se instaló previamente en las instancias de AWS.

Los intentos por forzar las autenticaciones son el objetivo de los servicios SSH todo el tiempo, y aunque el SSH ofrece una mayor protección que el RDP (por ejemplo, mediante la autenticación de 2 factores), si el servicio no se configura adecuadamente, fácilmente podría proporcionarle acceso a un actor malicioso. Los ataques para forzar el SSH y RDP, en conjunto, representaron hasta el 12% de todos los ataques registrados en los 'honeypots' del IoT de Kaspersky durante la primera mitad del 2019[1].

Las nubes públicas pueden exponerlo (y de hecho lo hacen) a vulnerabilidades, a continuación se muestran algunos ejemplos de cómo una vulnerabilidad en el software de terceros le brinda a un atacante la oportunidad para ejecutar su código en la propia instancia.

El 3 de junio del 2019 se descubrió una vulnerabilidad en Exim, un popular servidor de correo electrónico que con frecuencia se implementa en las nubes públicas. Esta vulnerabilidad permitió la ejecución remota de códigos. Si el servidor se ejecutó bajo el programa principal, como es el caso más común, entonces el código malicioso introducido en el servidor se ejecutaría con los privilegios del administrador[2].

Otro ejemplo es el hackeo del 2016 que se realizó en el sitio web oficial de Linux Mint. Esto resultó en la modificación de los puntos de distribución para incluir una "puerta trasera" IRC con la funcionalidad de DDOS. El troyano también podría utilizarse para depositar cargas maliciosas en los equipos infectados.

También hubo casos de módulos node.js maliciosos, contenedores infectados en el Docker Hub[3] y muchos otros. Los cibercriminales son muy ingeniosos cuando se trata de encontrar puntos de entrada a las infraestructuras, especialmente donde existen muchas infraestructuras de este tipo, todas muy parecidas y con problemas similares, y a todas ellas convenientemente se les considera altamente seguras por su diseño, de modo que no necesitan ninguna protección adicional.

Más de la mitad de todas las cargas de trabajo en las nubes públicas se ejecutan en Linux, y desafortunadamente existe el mito de que dichas cargas de trabajo son impenetrables para los atacantes.

Pero las vulnerabilidades, los módulos comprometidos y los scripts maliciosos realmente existen en los entornos de Linux. Estas son las estadísticas sobre las amenazas en Linux de nuestro laboratorio antimalware:

Amenaza	**%** de usuarios afectados
Vulnerabilidades	**41%**
Encubiertos	**24%**
Troyanos	**14%**
Otros	**21%**

1 https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

2 https://www.bleepingcomputer.com/news/security/critical-exim-tls-flaw-lets-attackers-remotely-execute-commands-as-root/

3 https://www.helpnetsecurity.com/2019/04/29/docker-hub-breach/

Vulnerabilidades en la seguridad y ataques en las nubes públicas

¿Qué puede hacer un actor malicioso una vez que está dentro de su infraestructura en la nube? Además de obtener acceso a los recursos de la empresa, como los datos de los clientes, básicamente podrán aprovechar los mismos beneficios de la nube pública que usted utiliza: escalabilidad instantánea, automatización y capacidad de configuración. Y todo eso a costa suya.

Caso 0: Tenemos un problema

Incluso si un cibercriminal no hace nada después de obtener acceso a uno de sus sistemas, usted sigue teniendo un problema: fue víctima de una vulneración. En muchos países del mundo, si se accede a un sistema que trabaja con datos importantes, protegidos o confidenciales, la ley exige que usted informe a las autoridades de la vulneración, así como la reparación de cualquier daño causado.

Los costos indirectos de la corrección por la vulneración de datos frecuentemente serán superiores a los costos directos, mientras que los efectos generalmente son mucho más duraderos. Y si la máquina comprometida se utiliza como un trampolín, es decir, una base para moverse lateralmente, vigilar, localizar y extraer información privilegiada de la cuenta o recopilar y extraer datos, las consecuencias para usted podrían ser terribles.

Piense en lo siguiente:
Pagar por la minería encubierta esencialmente es transferir dinero a la cuenta de un cibercriminal. No financie sus actividades comerciales a costa de las suyas.

Caso 1: Ataque basado en servicios SSH/RDPIf attackers have SSH

Si los atacantes tienen acceso SSH a un dispositivo infectado, tendrán muchas más posibilidades de monetizar la infección. En la abrumadora mayoría de los casos que involucran sesiones interceptadas que Kaspersky investigó, encontramos correos no deseados, intentos para usar nuestra honeytrap como un servidor proxy, y (por último, pero no por ello menos importante) minería de criptomonedas4. De hecho, registramos más de 50,000 intentos para infectar los entornos de Windows Server con mineros durante la primera mitad del 2019.

Entonces, ¿cómo puede prevenir estos ataques?

La solución

Una protección efectiva en la nube pública sería capaz de abordar casos como este desde varios frentes:

·El control de aplicaciones en el modo de rechazo predeterminado negaría automáticamente los permisos para que el software del atacante se implemente o se active
·La protección durante el tiempo de ejecución evitaría cualquier secuestro de recursos cuando se inicie el software
·La protección del comportamiento detectaría el software de minería, generadores de spam o cualquier otro software malintencionado, basándose en su comportamiento

Caso 2: Perder una gran cantidad de dinero en muy poco tiempo

La escalabilidad y la automatización instantánea significan que los cibercriminales que no están preocupados por mantenerse en el radar pueden volverse locos con su presupuesto. Una hora de uso en la instancia de AWS cuesta entre 5 centavos y 5 dólares, es decir, hasta $125 al día por instancia. Y no existe un límite en la cantidad de instancias que su atacante puede utilizar en su nombre. Pueden utilizar plantillas de formación de nubes para automatizar la generación de nuevos cálculos en la nube con el fin de realizar una tareacomo la minería de criptomonedas o DDOS. El atacante solo necesita crear nuevas instancias un poco más rápido de lo que usted puede desactivarlas. No es imposible perder $14K en un día [5] o incluso $50K o $60K[6]. O podría encontrarse aparentemente enviando un ataque DDOS, o convirtiéndose en sujeto de uno[7]...

La solución

Una solución de seguridad efectiva podría ayudarle en varios frentes:

·Visibilidad - Un motor de alertas y sistemas de informes adecuados le avisarían inmediatamente al administrador sobre el aumento de instancias
·Control de acceso a Internet – puede implementarse una política para evitar nuevas instancias y comunicaciones con los servidores de C&C, así como para evitar ataques en la red de salida

Caso 3: Ataque a la cadena de suministros

Los entornos construidos a partir de muchas fuentes ofrecen muchas opciones posibles cuando se trata de atacar la cadena de suministros del software, incluyendo la contaminación del depósito de Linux. Un ejemplo de esto, MeDoc, una empresa ucraniana, sufrió un ataque en sus mecanismos de actualización[8]. Las actualizaciones comprometidas se utilizaron para enviar un ataque basado en ExPetr, el limpiador de ransomware dirigido a las plataformas de Windows, el cual afectó a muchas empresas, entre ellas el gigante farmacéutico Merck, la

empresa de transporte marítimo Maersk y las infraestructuras críticas de Ucraniana.

4 https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/
5 https://dev.to/juanmanuelramallo/i-was-billed-for-14k-usd-on-amazon-web-services-17fn
6 https://www.quora.com/My-AWS-account-was-hacked-and-I-have-a-50-000-bill-how-can-I-reduce-the-amount-I-need-to-pay
7 https://www.reddit.com/r/aws/comments/3qt4e0/so_i_was_ddosed_by_35924_amazon_aws_ip_addresses
8 https://securelist.com/schroedingers-petya/78870/
https://securelist.com/in-expetrpetyas-shadow-fakecry-ransomware-wave-hits-ukraine/78973/
https://www.npr.org/sections/thetwo-way/2017/06/27/534560169/large-cyberattack-hits-ukraine-snarling-electric-grids-and-airports

La solución

Incluso si el malware llega como parte de una actualización al sistema protegido, debe tratarse exactamente como cualquier otro ejecutable o script, analizarse antes de que se ejecute y supervisarse durante su ejecución. El control de aplicaciones en modo de negación predeterminado puede agregar una capa adicional de seguridad.

Caso 4: Desde DevOps hasta la seguridad en DevOps

El malware y las vulnerabilidades incrustadas en las imágenes del contenedor pueden provocar filtraciones en el IP de la empresa o sabotajes en la línea de producción. El ataque a MeDoc que vimos anteriormente es un ejemplo, en otro, se cree que los hackers comprometieron el entorno de compilación de CCleaner para insertar malware[9] en los puntos de distribución oficiales del producto de seguridad.

La solución

Los equipos de DevOp que trasladan las implementaciones hacia la nube, y emplean entornos y herramientas dinámicas como los contenedores, necesitan reconocer el riesgo y administrarlo, al proteger el entorno de implementación basado en la nube.

Nuestra propia solución de seguridad específica en la nube, Kaspersky Hybrid Cloud Security, brinda protección durante el tiempo de ejecución a los servidores Docker para garantizar que las prácticas de implementación sean seguras. La API y otras herramientas también están disponibles para la automatización durante la implementación y la integración en el procesoCI/CD.

¿Por qué esto debería importarle?

Durante la primera mitad del 2019, evitamos más de 250,000 ataques en las plataformas de Windows Server de nuestros usuarios. Eso sin contar el AdWare y RiskWare.

La seguridad de una instancia en la nube pública es su responsabilidad, como le indicará cualquier proveedor de nubes públicas[10,11]. Eso es un hecho.

Es poco probable que su proveedor de la nube pública se haga responsable por las consecuencias de cualquier vulnerabilidad en la seguridad en términos de costos o daños a su marca o imagen pública.

Y además de eso, no existe límite en los volúmenes de la capacidad informática que un atacante podría obtener en su nombre, sin su conocimiento. Una vez más, usted sería responsable de cubrir los costos.

¿Realmente necesita un AV en una nube pública?

AWS cree que sí. Su consejo es el siguiente:

"Cree una configuración básica para el servidor donde incorpore parches de seguridad actualizados y conjuntos de protección basados en el servidor, los cuales incluyan antivirus, antimalware, detección/prevención de intrusiones y supervisión de la integridad de los archivos".

"Cada instancia de EC2 debe cumplir con los estándares de seguridad de la empresa. No instale funciones y características de Windows que no sean necesarias, e instale software para protegerse contra los códigos maliciosos (antivirus, antimalware, reducción de vulnerabilidades), supervise la integridad del servidor y realice la detección de intrusiones. Configure el software de seguridad para que le permita supervisar y mantener la configuración de seguridad del sistema operativo, proteger la integridad de los archivos críticos del sistema operativo y alertar sobre anomalías básicas en la seguridad".[12]

También creemos que si protege los sistemas operativos de sus instancias y máquinas virtuales, esto le permitiría reducir y administrar los riesgos de una forma mucho más eficiente. La protección contra malware y antivirus básica claramente no es suficiente. Las prácticas recomendadas de la industria dictan que todos los sistemas operativos de una infraestructura necesitan de una protección multicapa e integral, y los proveedores de la nube pública hacen recomendaciones similares.

Aquí es donde actúa una solución de seguridad como Kaspersky Hybrid Cloud Security. Nuestra solución protege diferentes tipos de cargas de trabajo que se ejecutan en diferentes plataformas, ya que utiliza tecnologías de seguridad en varios niveles, incluyendo el fortalecimiento del sistema, prevención de vulnerabilidades, supervisión de la integridad de los archivos, un bloqueador contra los ataques en la red, antimalware estático y de comportamiento, y muchas cosas más.

Es esencial que garantice la aplicación de los niveles de seguridad adecuados para su entorno de nube pública en todo momento, para evitar ataques que podrían resultar extremadamente costosos y perjudiciales. Es importante que reconozca la seguridad como un elemento fundamental para su estrategia continua en la nube. Después de todo, en última instancia, ¡es su problema!

9 https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that-corrupted-ccleaner/

10 https://aws.amazon.com/compliance/shared-responsibility-model/

11 https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure

12 https://aws.amazon.com/answers/security/aws-securing-windows-instances/

www.kaspersky.com

Kaspersky Hybrid Cloud Security para AWS: kaspersky.com/aws
Kaspersky Hybrid Cloud Security para Azure: kaspersky.com/azure
Kaspersky Hybrid Cloud Security: kaspersky.com/hybrid

#hybrid
#aws_instance_security
#azure_vm_security