FORTINET
NSE Training Institute

NSE 2 Cloud Security Scripts—Spanish Version

¡Hola! En esta lección, exploramos la misteriosa "nube", lo que realmente es, cómo surgió y algunos de los problemas de seguridad que encontramos allí.

Primero, desmitifiquemos la nube. Es gracioso que "la nube" tenga un reconocimiento de nombre público extremadamente alto, pero pocos entienden lo que realmente es.

Tradicionalmente, antes de la nube, las empresas y otras organizaciones compraban sus propios sistemas informáticos para ejecutar el software de aplicación necesario que les permitiese desarrollar el negocio. Estos sistemas informáticos estaban ubicados en las instalaciones de la compañía y administrados por equipos de empleados. Sin embargo, no siempre era así, a menudo había más de un sistema informático (o servidor) por cada aplicación principal.

Esta configuración era costosa debido al costo de capital del hardware de la computadora y el costo de mano de obra de las personas que lo mantenían funcionando. Estos sistemas aumentaban la productividad general y ayudaban a mantener una ventaja competitiva.

Recientemente, alguien notó que, de todos sus sistemas informáticos, solo algunos estaban completamente ocupados en ciertos momentos. La mayoría estaban inactivos, esperando que la próxima transacción entrara. En pocas palabras: había muchos recursos desperdiciados.

Entonces, se desarrolló una nueva forma de usar el hardware del servidor llamada **Virtualización**. Un modelo que proviene de la tecnología antigua en la informática de mainframe que permite que un solo servidor ejecute los sistemas operativos y las aplicaciones desde múltiples servidores simultáneamente. La virtualización consolida las cargas de trabajo en menos servidores, lo que aumenta su utilización y ahorra dinero.

Poco tiempo despues, la mayoría de los centros de datos se transformaron de filas de hardware informáticos dedicadas a aplicaciones específicas, en una colección –o

grupo– de recursos de hardware generales que ejecutan aplicaciones virtualizadas. Era lo más inteligente que se podía hacer.

Después vinieron algunos empresarios visionarios que construyeron enormes centros de datos, llenos de sistemas informáticos generalizados, que ofrecieron alquilar parte de esta infraestructura para que sus clientes pudieran ejecutar sus aplicaciones virtualizadas, en lugar de hacerlo en su propio hardware. Es así como nació la nube.

Este tipo de computación en la nube se denomina Infraestructura como Servicio o IaaS. IaaS proporciona a las organizaciones las soluciones de redes, almacenamiento, servidores físicos y virtualización, mientras que los usuarios deben seguir proporcionando computadoras con sistemas operativos, middleware, datos y aplicaciones. El middleware es un software que actúa como puente entre el sistema operativo y las aplicaciones. Las organizaciones utilizan este tipo de servicio cuando la demanda de sus servicios o productos varía, por ejemplo, durante las temporadas en las que aumentan las cargas de trabajo de los sistemas. Algunos ejemplos de estos proveedores de servicios son Amazon Web Services, Microsoft Azure y Google Compute Engine.

También existen otros tipos de nubes. Por ejemplo, los proveedores de servicios alquilan plataformas basadas en la nube para que los desarrolladores de software produzcan y distribuyan aplicaciones. Este servicio, denominado Plataforma como Servicio o PaaS, proporciona el sistema operativo y middleware, además de los elementos proporcionados por la IaaS. Un servicio que facilite las cosas hace más eficiente y rentable la creación, prueba e implementación de aplicaciones para las organizaciones.

Un tercer ejemplo es el Software como Servicio o SaaS. En este servicio en la nube, un tercero se encarga de alojar el software. Normalmente, el usuario final se conecta a la aplicación mediante su explorador. Algunos ejemplos comunes de aplicaciones disponibles a través de SaaS son Google Mail, Salesforce, DocuSign y Netflix.

De cualquier manera, resulta muy atractivo para la mayoría de las organizaciones trasladar el costo de las aplicaciones que se ejecutan en activos de capital de hardware y propiedad de la compañía a un modelo donde el precio es un costo operativo.

Ahora veamos qué significa esto para la seguridad.

Cuando las aplicaciones se alojan en el propio centro de datos de una empresa, el despliegue de seguridad es sencillo: colocar la tecnología de seguridad adecuada en los lugares correctos para abordar los problemas de seguridad específicos.

Proporcionar seguridad para la nube, por su parte, no es tan claro. Se podría decir que está un poco nublado. En pocas palabras, la seguridad es una **responsabilidad compartida** entre el proveedor de la nube y el cliente que utiliza los servicios de la nube.

Diseñada en capas, la seguridad incluye los componentes físicos y componentes lógicos.

La infraestructura en la nube proporcionada por los proveedores de IaaS está protegida de varias maneras. Desde el punto de vista de la disponibilidad, la infraestructura está diseñada por el proveedor para estar altamente disponible, y se deduce que el tiempo de actividad de la infraestructura es responsabilidad del proveedor. Desde el punto de vista de la seguridad, el proveedor solo es responsable de proteger la infraestructura que proporciona.

Como cliente, cuando instala una o más aplicaciones virtualizadas en la infraestructura de nube del proveedor, él se hace responsable de asegurar el acceso, el tráfico de red y los datos de las aplicaciones.

Ahora, la mayoría de los proveedores suministran algún tipo de herramientas de seguridad para asegurar varias partes del entorno de aplicaciones en la nube del cliente. Sin embargo, estas herramientas pueden plantear algunos problemas.

Primero, estas herramientas tienden a proporcionar solo unas pocas funciones básicas de seguridad y son las mismas herramientas que utiliza el proveedor para proteger la infraestructura subyacente. Si un atacante traspasara estas herramientas en la capa de infraestructura, probablemente también podría traspasarlas en el nivel de aplicación del cliente.

En segundo lugar, y quizás más importante, es el hecho de que muchas organizaciones operan en un mundo híbrido donde algunas de sus aplicaciones permanecen alojadas en sus propios centros de datos, algunas en la plataforma en la nube IaaS del vendedor A, algunas en la plataforma en la nube del vendedor B y otras con múltiples vendedores de SaaS. Esto es lo que llamamos un entorno "Multi-Cloud", y viene con múltiples problemas: soluciones de seguridad múltiples, independientes y descoordinadas, un problema donde la complejidad puede escalar geométricamente con el número de proveedores de la nube involucrados.

Además, el personal de seguridad altamente capacitado es escaso. Agregue a eso una carga para integrar y operar múltiples entornos de seguridad no integrados simultáneamente ... puede ser un problema real.

En Fortinet, tenemos soluciones de seguridad como FortiGate, FortiMail, FortiWeb, FortiSandbox, FortiInsight y otras dentro del Fortinet Security Fabric, que no solo se encuentran en el centro de datos de la empresa, brindando la misma seguridad constante, sino que están optimizadas para todos los proveedores de nube líderes de IaaS como AWS de Amazon, Microsoft Azure, Google Cloud, VMware, Cisco ACI, Oracle Cloud e IBM.

Para concluir, hemos mostrado los fundamentos de cómo surgió "la nube", cómo se protegen los entornos en la nube, y describimos la estrategia de seguridad en la nube de Fortinet que se desenvuelve y escala desde entornos simples solo en la nube, hasta entornos complejos en varias nubes.

Gracias por su tiempo y recuerde realizar la prueba al finalizar esta lección.