

TOP 3 CONSIDERACIONES PRINCIPALES PARA LA SEGURIDAD EN LA NUBE

Un centro de datos es un entorno fijo en el que las aplicaciones se ejecutan en servidores dedicados a los que solo pueden acceder usuarios autorizados.

En contraste, un entorno de la nube es dinámico y automatizado, donde hay grupos de recursos informáticos disponibles para soportar las cargas de trabajo de las aplicaciones, a las que se pueden acceder desde cualquier ubicación, en cualquier momento, desde cualquier dispositivo. Para el profesional de seguridad de información experimentado, parece que muchos de los principios que hacen que la informática de la nube sea atractiva van en contra de las mejores prácticas de seguridad de la red. A continuación, se enumeran las tres consideraciones principales para proteger los centros de datos tradicionales y aquellos basados en la nube, así como los requisitos clave para la seguridad en la nube.

La Informática de la Nube No Disminuye los Riesgos de Seguridad de Red Existentes

Los riesgos de seguridad que amenazan un centro de datos y una red actualmente cambian una vez que las aplicaciones se mueven a la nube, ya sea en una migración completa o en un escenario híbrido, en el que algunas aplicaciones se mueven a la nube mientras que otras permanecen en las instalaciones. De hecho, en varias maneras, los riesgos de seguridad que se enfrentan al moverse a la nube se vuelven más significativos.

Por ejemplo, muchas aplicaciones de centros de datos usan un amplio rango de puertos, lo que hace que muchas de las medidas de seguridad tradicionales sean ineficaces cuando esas aplicaciones se mueven a la nube. Los cibercriminales están creando ataques sofisticados independientes de los puertos que usan múltiples vectores para comprometer su objetivo, se esconden a plena vista y utilizan aplicaciones comunes para completar su misión.

La Seguridad Quiere Separación y Segmentación - La Nube Confía en Recursos Compartidos

Por décadas, las mejores prácticas de seguridad de la información dictaron que las aplicaciones cruciales para la misión y los datos sean separados en segmentos seguros en la red. Generalmente, a esto se lo llama Confianza Cero: nunca confiar, siempre verificar.

En una red física en el centro de datos empresarial, Confianza Cero es un método relativamente directo para implementarse a través del uso de firewalls y VLANs (es decir, LANs virtuales), gestionados por políticas basadas en aplicaciones e identidad de usuario.

INFORMACIÓN Y CONOCIMIENTOS

En un entorno informático de la nube, la comunicación directa entre máquinas virtuales en un servidor ocurre constantemente, en algunos casos en varios niveles de confianza. Esto hace que la segmentación sea una tarea difícil, especialmente debido a que las aplicaciones de la nube se basan en la noción de recursos compartidos. Los niveles de confianza mezclados, al combinarse con una falta de visibilidad del tráfico dentro del host por las ofertas de seguridad basadas en puertos virtualizados, presentarán probablemente una postura de seguridad debilitada.

Las Configuraciones de Seguridad Están Orientadas hacia el Proceso | Los Entornos de la Informática de la Nube Son Dinámicos

Las cargas de trabajo virtuales se pueden crear o modificar en minutos. Como tal, los equipos de informática de la nube operan en un entorno altamente dinámico, con cargas de trabajo agregándose, eliminándose y cambiando constantemente.

Por el contrario, la configuración de seguridad para esta carga de trabajo puede llevar horas, días o semanas. Las demoras de seguridad no están diseñadas para crear controles. En lugar de eso, son el resultado de un proceso que está diseñado para mantener una postura de seguridad sólida. Los cambios en las políticas deben ser aprobados, se deben identificar los firewalls apropiados y se deben determinar las actualizaciones de las políticas relevantes.

A menos que se entienda este desequilibrio y se lidie con él como parte de la migración de la nube, el resultado es una discrepancia entre las políticas de seguridad y la implementación de las cargas de trabajo de la nube. El resultado es una postura de seguridad debilitada que puede poner en peligro datos y propiedad intelectual importante y, quizás también, puede generar rupturas en el cumplimiento y la implementación de políticas y regulaciones.

Requisitos Clave para Asegurar la Nube

- **Seguridad consistente** en factores de forma físicos y virtualizados. Se necesitan los mismos niveles de control de aplicaciones, manejo de aplicaciones fraudulentas y mal configuradas, y prevención de amenazas para proteger el entorno informático de la nube y de la red física.
- **Segmentar** aplicaciones comerciales bajo los principios de Confianza Cero. Para poder maximizar completamente el uso de los recursos informáticos, ahora es una práctica relativamente común mezclar niveles de confianza de cargas de trabajo de las aplicaciones en el mismo recurso informático. El objetivo es controlar el tráfico entre las cargas de trabajo a la vez que se previene el movimiento lateral de amenazas.
- **Gestionar** la implementación de la seguridad y alinear las actualizaciones de las políticas de forma central. La seguridad de la red física aún se implementa en casi todas las organizaciones, así que es crucial tener la habilidad de gestionar las implementaciones de hardware y de factores de forma virtual desde una ubicación centralizada con la misma infraestructura e interfaz de gestión. La solución seleccionada debe ser capaz de abarcar los entornos físicos y virtuales a través de una gestión de políticas y un marco de aplicación consistentes, y debe incluir características que automatizan las actualizaciones de las políticas de seguridad.

Para conocer más sobre cómo asegurar los centros de datos tradicionales y los centros de datos basados en la nube con firewalls de nueva generación, lea la [documentación técnica](#).



¿Quieres mejorar tu estrategia de Seguridad en la Nube?

Asesoría Gratis

APRENDE CÓMO TRANSFORMAR TU ESTRATEGIA DE CIBERSEGURIDAD Y AUMENTAR LA PROTECCIÓN DE TU INFORMACIÓN, SERVICIOS Y APLICACIONES EN LA NUBE

