4. Valoración de Servicios Cloud

4.1.3. Beneficios y Riesgos de los Servicios en Cloud (III).

Aparte del análisis de principales riesgos y beneficios según el tipo de servicio IaaS, PaaS, SaaS y la seguridad, cabe ampliar el análisis según aspectos más específicos como las interfaces de acceso, o las facilidades de escalado, veamos estos.

INTERFACES NORMALIZADAS PARA SERVICIOS DE SEGURIDAD GESTIONADOS

El tener que adaptarse a ciertas configuraciones predefinidas, como un panel de control, puede no ser un problema, ya que los grandes proveedores en nube pueden ofrecer una interfaz abierta y estandarizada a los proveedores de servicios de seguridad gestionadas que ofrecen servicios a todos sus clientes de un modo muy accesible.

Potencialmente, ello genera un mercado más abierto y disponible de servicios de seguridad, donde los clientes pueden cambiar de proveedor con mayor facilidad e incurriendo en menores gastos de configuración.

ESCALADA RÁPIDA E INTELIGENTE DE RECURSOS

¿Y qué pasa ante un ataque como el de denegación de servicio (DDoS)? La lista de recursos en nube que pueden ser escalados rápidamente bajo demanda ya incluye, entre otros, el almacenamiento, el tiempo de CPU, la memoria, las solicitudes de servicios web y las máquinas virtuales, y el nivel de control granular sobre el consumo de recursos aumenta a medida que las tecnologías mejoran.

Un proveedor en nube tiene potencial para reasignar recursos de manera dinámica para el filtrado, la catalogación de tráfico, la codificación, etc., con vistas a incrementar el apoyo a las medidas defensivas ante un ataque DDoS cuando un ataque está produciéndose o consideremos que puede producirse.

Cuando esta capacidad de reasignación dinámica de recursos se combina con métodos adecuados de optimización de recursos, el proveedor en nube puede limitar las posibles consecuencias de determinados ataques sobre la disponibilidad de los recursos que utilizan los servicios alojados legítimamente, así como reducir el impacto del incremento de uso de los recursos por la defensa de seguridad para hacer frente a dichos ataques.

Sin embargo, para lograr este efecto, el proveedor debe aplicar una coordinación adecuada de la autonomía para la defensa de seguridad y para la gestión y optimización de los recursos.

La capacidad de escalar dinámicamente los recursos defensivos bajo demanda posee ventajas evidentes con respecto a la resistencia a los fallos. Además, cuanto mayor sea la escalada de los distintos tipos de recursos individuales de manera granular —sin escalar la totalidad de los recursos del sistema—, más barato será responder a los picos repentinos (no maliciosos) de demanda.

Cómo obtener lo mejor del cloud

La consideración de los beneficios y riesgos no debe ocultarnos el importante hecho de que la nube ofrece a los integradores, y en consecuencia a los usuarios, una oportunidad enorme para pasar de un negocio basado en servicios a gestionar su propia infraestructura y ampliar su atractivo para los clientes.

Para ello, cuando se seleccione un partner para el centro de datos, el proveedor de servicios debe también considerar qué soporte y SLA le ofrecen, pues esto tendrá un impacto que limitará lo que a su vez podrá ofrecer a sus clientes.

Dado que el cloud busca ofrecer un servicio o una aplicación, la mejor forma de monitorizar su rendimiento es definir métricas que estén basadas en el rendimiento y la disponibilidad de lo ofrecido.

Obtener lo mejor de la nube requiere planificación, una selección cuidadosa de los partners y asegurarse de que se cuenta con la infraestructura más adecuada para dar soporte al negocio. En última instancia, el Acuerdo de Nivel de Servicio respaldará la fiabilidad de dichos servicios. Aspectos que consideramos en la próxima lección.

Referencias:

- Cloud Computing. Benefits, risks and recommendations for information security. Págs. 23-25