5. Implantación y migración a servicios cloud

5.1.2. Fijación de Objetivos e Identificación de Riesgos (II).

Continuamos con el análisis de aspectos que nos ayudan a identificar riesgos, y su gestión, en el proceso de implantación y migración a servicios cloud

COMPROMISO DE CONTROL EN LA INTERFAZ DE GESTIÓN
Las interfaces de gestión de cliente de un proveedor en nube público son accesibles a través de Internet, y canalizan el acceso a conjuntos de recursos más grandes (que los proveedores tradicionales de alojamiento), por lo que plantean un riesgo mayor, especialmente cuando son combinados con el acceso remoto y las vulnerabilidades del navegador de web.

LA PROTECCIÓN DE DATOS
La computación en nube plantea varios riesgos relativos a la protección de datos tanto para clientes en nube como para proveedores en nube. En algunos casos, puede resultar difícil para el cliente en nube comprobar de manera eficaz las prácticas de gestión de datos del proveedor en nube, y en consecuencia, tener la certeza de que los datos son gestionados de conformidad con la ley. Este problema se ve exacerbado en los casos de transferencias múltiples de datos.

Por otra parte, algunos proveedores en nube sí proporcionan información sobre sus prácticas de gestión de datos. Otros también ofrecen resúmenes de certificación sobre sus actividades de procesamiento y seguridad de datos y los controles de datos a que se someten.

SUPRESIÓN DE DATOS INSEGURA O INCOMPLETA
Cuando se realiza una solicitud para suprimir un recurso en nube, al igual que sucede con la mayoría de sistemas operativos, en ocasiones el proceso no elimina definitivamente los datos. En ocasiones, la supresión adecuada o puntual de los datos también resulta imposible (o no deseable, desde la perspectiva del cliente), bien porque existen copias adicionales de datos almacenadas pero no disponibles o porque el disco que va a ser destruido también incluye datos de otros clientes. La multiprestación y la reutilización de recursos de hardware representan un riesgo mayor para el cliente que la opción del hardware dedicado.

MIEMBRO MALICIOSO
Aunque no suelen producirse habitualmente, los daños causados por miembros maliciosos son, con frecuencia, mucho más perjudiciales. Las arquitecturas en nube necesitan ciertas funciones cuyo perfil de riesgo es muy elevado. Algunos ejemplos son los administradores de sistemas de proveedores en nube y los proveedores de servicios de seguridad gestionada.

Los riesgos enumerados anteriormente no siguen un orden de criticidad concreto, sino que simplemente constituyen algunos de los riesgos más relevantes de la computación en nube. Los riesgos del uso de la computación en nube deben ser comparados con los riesgos derivados de mantener las soluciones tradicionales, como los modelos de sobremesa.

A menudo es posible, y en algunos casos recomendable, que el cliente en nube transfiera el riesgo al proveedor en nube; sin embargo, no todos los riesgos pueden ser transferidos.

Si un riesgo provoca el fracaso de un negocio, perjuicios graves al renombre del mismo o consecuencias legales, es muy difícil, y en ocasiones, imposible, que un tercero compense estos daños. En última instancia, puede subcontratar la responsabilidad, pero no puede subcontratar la obligación de rendir cuentas.

Para la gestión de estos riesgos podemos adoptar herramientas o procedimientos como los siguientes:

AUDITORÍA Y RECOGIDA DE PRUEBAS

Si estamos en un caso de IaaS, esta permite la clonación de máquinas virtuales bajo demanda. En caso de supuesto incumplimiento de la seguridad, el cliente puede tomar una imagen de una máquina virtual activa —o de los componentes virtuales de la misma— para llevar a cabo un análisis forense fuera de línea, lo cual reduce el tiempo de espera para la realización el análisis.

ACTUALIZACIONES Y OPCIONES MÁS PUNTUALES, EFECTIVAS Y EFICACES

Las imágenes por defecto de las máquinas virtuales y los módulos de software utilizados por los clientes pueden ser reforzados y actualizados previamente con los últimos parches y configuraciones de seguridad, conforme a procesos ajustados; las API del servicio en nube de la IaaS también permiten tomar imágenes de la infraestructura virtual de manera frecuente y comparada con un punto inicial

LA AUDITORÍA Y LOS ACUERDOS DE NIVEL DE SERVICIO OBLIGAN A GESTIONAR MEJOR EL RIESGO

La frecuencia de las auditorías impuestas a los proveedores en nube tiende a exponer los riesgos que, de otro modo, no habrían sido identificados, con lo que tiene el mismo efecto positivo.

BENEFICIOS DE LA CONCENTRACIÓN DE RECURSOS

Aunque sin duda la concentración de recursos tiene desventajas para la seguridad, posee el beneficio evidente de abaratar la perimetrización y el control de acceso físicos y permite una aplicación más sencilla y económica de una política de seguridad exhaustiva y un control sobre

la gestión de datos, la administración de parches, la gestión de incidentes y los procesos de mantenimiento.

Referencias:

- Cloud Computing. Benefits, risks and recommendations for information security. Págs. 21-22