Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Análisis Forense Informático

UD03. Consideraciones Cloud.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico

La empresa de María va a contratar servicios de cloud para poder almacenar determinados datos de la empresa, están barajando distintas ofertas de los proveedores.

Tienen la preocupación de llegado el caso de un Incidente de seguridad si serán capaces de poder realizar los análisis forenses correspondientes. También tienen la duda de qué pasará con esos datos y si serán accesibles.

Para ello solicitan la ayuda de María para internamente saber cómo deben de gestionar el contrato con el proveedor de servicios.

¿Qué te pedimos que hagas?

✓ **Apartado 1: Consideraciones de la Nube**

Esta tarea es eminentemente teórica, para realizarla deberás **repasar los conceptos previamente explicados e investigar** sobre la protección de datos y regulaciones.

➢ Cuando una empresa contrata un servicio de cloud o nube, ¿qué consideraciones tiene que tener en cuenta y más teniendo en cuenta los aspectos de futuros forenses en este entorno?

- Habrá que decidir el tipo de nube más adecuado a las necesidades de la empresa (pública, privada o híbrida. El tipo de servicio (SaaS, IaaS o PaaS).
- Cumplimiento normativo adecuado a la normativa vigente de seguridad y privacidad, así como del RGPD. También que posea las debidas certificaciones de seguridad. Aunque esté en la nube, la empresa sigue siendo la responsable final de los datos.
- Conocer si intervienen en el contrato terceras partes para los servicios cloud, o cualquier otro punto relativo a la privacidad y seguridad de los datos.
- Medidas concretas de seguridad. Encriptación, detección y respuesta ante incidentes…
- Políticas de acceso y uso de los datos. Asegurar en contrato el control y acceso completo a los datos de la empresa.
- Asegurar que los servicios contratados tienen un plan de gestión ante incidentes.
- La localización física de los datos. Debe detallar ese aspecto para asegurar que se encuentran los servidores en la Unión Europea, y sino que justifique las garantías adecuadas para evitar cualquier tipo de problema por estar en otra jurisdicción.
- Opciones de copia de seguridad y recuperación de datos.
- Servicio con una comunicación clara y transparente acerca de todo lo tratado en las consideraciones anteriores.

➢ ¿Qué sucede si tenemos que hacer la investigación en un entorno o máquina que tenemos subcontratado a un proveedor que tiene los servicios en nube?

Nos comunicaremos con el proveedor para informarle de dicha investigación. Nos aseguraremos de poder acceder a los datos y al entorno, con la colaboración del proveedor (según lo dispuesto en el apartado anterior, estará en contrato).

Comprobaremos (también lo apuntamos en el apartado anterior) que la ubicación de los datos está dentro del ámbito de la Unión Europea o garantizado por regulación, para poder solicitar el acceso en el momento de la investigación, y asegurarnos la validez.

➢ ¿Qué obligaciones y responsabilidades tiene el cliente que contrata servicios de cloud a efectos de protección del dato?

Como ya apuntamos, la empresa es el responsable último respecto protección de los datos.

Tendremos obligaciones y responsabilidades como:

- Evaluación de los proveedores de servicios de cloud en términos de seguridad y protección de datos.
- Asegurar que se hay establecido un acuerdo de confidencialidad con el proveedor de servicios de cloud.
- Identificar y documentar la naturaleza, alcance, contexto y finalidad del tratamiento de datos personales.
- Garantizar el cumplimiento de las normas y regulaciones del RGPD por parte del proveedor de servicios de cloud.
- Establecer medidas de seguridad adecuadas.
- Garantizar la privacidad y seguridad de los datos personales.
- Supervisar y monitorear el cumplimiento de sus obligaciones respecto a protección de datos por parte del proveedor.
- Notificar a las autoridades competentes y a los interesados en caso de incumplimiento o violación de datos.
- Mantener un registro de las actividades de tratamiento de datos personales.
- Ejercitar los derechos de acceso, rectificación, eliminación y portabilidad de los datos personales.
- Cumplir con las obligaciones de transparencia y de información al titular de los datos.

➢ ¿Qué es un servicio transparente de cloud? ¿Qué consecuencias tiene un servicio opaco?

En un servicio transparente, el cliente tiene acceso a dónde, cuándo y quién ha almacenado, o accedido y procesado, los datos que mantiene alojados en el cloud, así como el control sobre configuración de seguridad y privacidad de los datos.

En un servicio opaco, perdemos el control preciso que tenemos con un servicio transparente, quedando en manos del proveedor.

Al ser la empresa la responsable final de los datos puede tener problemas al no poder asegurar el cumplimiento regulatorio y normativo de protección de datos, además de tener una posición comprometida en caso de incidente.

➢ ¿Cómo puedo recuperar mis datos? Y si son de carácter personal (art 20 RGPD)

Si hemos tomado las precauciones adecuadas por contrato tras el análisis del primer punto, deberemos poder acceder a nuestros datos (incluidos los de carácter personal) y el proveedor nos permitirá la portabilidad de los mismos (a servicios internos propios u otra nube).

- ¿Qué garantías debo pedir al proveedor de servicios de cloud para evitar tener problemas al hacer un forense en el entorno de cloud o nube?

  Como hemos apuntado en el primer punto, podremos exigir garantías de asistencia, ubicación, disponibilidad, integridad y confidencialidad de los datos alojados en el cloud, así como el acceso y herramientas de análisis compatibles.

- ¿Puedo pedir al proveedor que se convierta en el responsable de mis datos al tenerlos alojados en su nube?

  No. La empresa es la responsable última por ley. Da igual que se intente reflejar de otra forma en contrato. Podremos establecer cláusulas sobre el manejo de los datos, pero siempre a sabiendas de ser los responsables finales.

Webgrafía.

https://www.aepd.es/documento/guia-cloud-clientes.pdf

https://www.aepd.es/documento/guia-cloud-prestadores.pdf

https://www.protecciondatos.org/clausulas-contrato-cloud-computing/