1.- Realización de análisis forenses en Cloud.

Caso práctico

Pixabay (Dominio público)

María esta investigando un incidente de seguridad crítico debido a un ransomware que ha provocado la parada de producción en una gran empresa del Ibex35.

Durante la investigación se encuentra debido al análisis del tráfico de red y del forense de varias máquinas que el origen del ataque podría ser el acceso ilegitimo a una máquina en cloud siendo la vía de entrada a la empresa,

Necesita confirmar esta hipótesis pero para eso requiere hacer el forense de esta máquina que esta en la nube. Aunque está maquina esta en la nube pertenece a una empresa que les da servicios de nube, por lo que antes de solicitar hacer el forense necesita ver en que localizaciones está la empresa, la máquina, el servicio que dan...ya que sino podría tener problemas legales y la evidencia podría no ser válida en juicio.

Los servicios basados en la nube han cambiado la forma en que muchas empresas hacen negocios. Al adoptar la migración a la nube, las empresas pueden alojar su software y aplicaciones en servidores económicos, ahorrándoles tiempo, dinero y los gastos y molestias de administrar hardware dedicado.

Estos servicios también permiten que las empresas y las personas almacenen una gran cantidad de datos de forma segura. Las tecnologías basadas en la nube son convenientes y económicas, pero el análisis forense de la nube es un problema que todo propietario de una empresa debe revisar antes de implementar estas estrategias en los procesos cotidianos.

1.1.- Nube privada y nube pública o híbrida.

Pixabay (Dominio público)

Cuando hablamos de entornos ***cloud*** o de nube deberemos de tener en cuenta que existen varios tipos de nube según su arquitectura y tipología y que por ende condicionaran nuestro análisis forense.

Nube pública
Las empresas que utilizan la nube pública para sus aplicaciones contratan a un proveedor de servicios en la nube para almacenar sus datos fuera de la empresa. Pueden acceder a software, redes y servidores en cualquier momento desde cualquier dispositivo. La empresa comparte esta nube con otros clientes del proveedor.

Si bien compartir la misma infraestructura informática con otros clientes del proveedor puede resultar rentable a nivel de costes, la empresa tiene poco control sobre la seguridad de los datos. No se recomienda una nube pública para las empresas que almacenan datos confidenciales o necesitan cumplir con ciertas regulaciones de manejo de datos. Si hay que realizar un forense de una evidencia de esta nube tendremos que legislación vigente según la localización física del servidor y solicitarlo al proveedor (según el tipo de servicio ofrecido).

Nube privada
Con una nube privada, una empresa implementa sus propios servicios y almacenamiento basados en la nube, generalmente en las propias instalaciones o centros de datos de la empresa. La empresa es responsable de desarrollar sus propias aplicaciones e infraestructura y de administrar sus propios datos y seguridad.

Por lo general, esta es ,en términos generales, la opción más costosa y la mejor para las empresas que deben cumplir con ciertas regulaciones de almacenamiento de datos. Los investigadores forenses que necesiten analizar una evidencia en esta nube tienen acceso a todos los datos y a toda la infraestructura, por lo que puede ser útil si surge un problema.

Nube híbrida
Con una nube híbrida, los datos que una empresa almacena en la nube se dividen entre almacenamiento público y privado. La empresa puede almacenar sus datos confidenciales en su propia nube privada, pero permitir que el resto de la infraestructura se almacene en la nube pública.

La nube híbrida permite a las empresas ahorrar dinero en sus servicios basados en la nube y, al mismo tiempo, proteger los datos privados. Sin embargo, el proveedor de servicios en la nube aún posee los datos almacenados en la nube pública, lo que puede dificultar que los investigadores forenses en la nube hagan su trabajo después de una violación de datos.

Para saber más

Los tipos de servicios que una empresa o individuo elige implementar dependerán en última instancia de sus objetivos y necesidades. Podían elegir entre servicios en la nube SaaS, PaaS o IaaS .

SaaSCuando un usuario o empresa busca productos finales o herramientas en la nube (aplicación de correo electrónico, programas de cálculo, etc) puede contratar servicios de Software como Servicio (valga la redundancia) desde una plataforma SaaS (*Software as a Service*), el software y todos sus datos relacionados permanecen en la nube. La empresa que vende en el mercado SaaS permite que la aplicación se aloje en la nube. **Por lo tanto, el proveedor es responsable de administrar el contenido y los datos del software.**

IaaSCuando un usuario o empresa busca almacenamiento y procesamiento en bruto en la nube puede contratar servicios de IaaS (Infraestructura como servicio), su infraestructura informática está alojada por un proveedor de nube externo. **El proveedor es propietario de su red y almacenamiento, pero la empresa sigue siendo parcialmente responsable de la integridad de los datos, las aplicaciones y el sistema operativo que se utiliza en la IaaS.**

PaaSA medio camino entre las dos últimas aproximaciones está Paas

(Plataforma como Servicio). Surge de la necesidad de las empresas para construir aplicaciones que serán más tarde usadas como herramientas por los usuarios. Como propietaria de la plataforma PaaS, la empresa es responsable de los datos y las aplicaciones que contiene, pero no del almacenamiento, la red, los servidores o el sistema operativo.

Debes conocer

Durante las investigaciones forenses los analistas pueden encontrarse que sus evidencias no son accesibles o no se consideran válidas debido a temas regulatorios. Una de las principales leyes federales de EEUU es la conocida como "Ley Patriot". Puedes encontrar mas información aquí

1.2.- Retos legales, organizativos y técnicos particulares de un análisis en Cloud.

Aunque un análisis de un entorno cloud a nivel técnico no cambia mucho de un entorno local si que puede tener cambios significativos en cuanto la legalidad, validez y propiedad del dato que podrían hacer que el proceso de extracción de evidencias se complicase.

A principios de 2018 se promulgaron dos leyes relacionadas con la protección y la privacidad de los datos: la Ley estadounidense Clarifying Lawful Overseas Use of Data (CLOUD) y el Reglamento General de Protección de Datos (GDPR) de la UE. Estas leyes (sobre todo GDPR) condicionan los procesos de extracción de evidencias, propiedad y responsabilidad de los datos y la validez del proceso y evidencias en un juicio. Por ejemplo en la UE la ubicación del dato es de vital importancia a efectos regulatorios.

Pixabay (Dominio público)

Si hay una violación de datos u otro tipo de delito digital, los investigadores forenses necesitan acceso a todas las pruebas para ayudar a resolver el delito. Esta evidencia también debe ser admisible en juicio para acusar a los responsables.

Las infraestructuras en la nube podrían dificultar estas investigaciones porque es posible que las empresas víctimas no posean todos los datos o pruebas. Si está alojado en una jurisdicción diferente, es posible que no sea admisible. Es posible que los usuarios o incluso los investigadores forenses tampoco tengan control sobre si terceros (proveedores, gobiernos, otros analistas forenses) manipulan sus datos, ya que no son los únicos propietarios de esos datos en una nube pública.

Para saber como resolver los problemas que pudieran derivar tenemos que saber qué modelo de nube tenemos, que servicios realmente tenemos contratados (ver más abajo) y qué jurisprudencias podrían aplicar sobre la responsabilidad y propiedad del dato.

Debes conocer

Los tipos de servicios que una empresa o individuo elige implementar dependerán en última instancia de sus objetivos y necesidades. Podían elegir entre servicios en la nube SaaS, PaaS o IaaS .

SaaSCuando un usuario o empresa busca productos finales o herramientas en la nube (aplicación de correo electrónico, programas de cálculo, etc) puede contratar servicios de Software como Servicio (valga la redundancia) desde una plataforma SaaS (Software as a Service), el software y todos sus datos relacionados permanecen en la nube. La empresa que vende en el mercado SaaS permite que la aplicación se aloje en la nube. Por lo tanto, el proveedor es responsable de administrar el contenido y los datos del software.

IaaSCuando un usuario o empresa busca almacenamiento y procesamiento en bruto en la nube puede contratar servicios de IaaS (Infraestructura como servicio), su infraestructura informática está alojada por un proveedor de nube externo. El proveedor es propietario de su red y almacenamiento, pero la empresa sigue siendo parcialmente responsable de la integridad de los datos, las aplicaciones y el sistema operativo que se utiliza en la IaaS.

PaaSA medio camino entre las dos últimas aproximaciones está Paas (Plataforma como Servicio). Surge de la necesidad de las empresas para construir aplicaciones que serán más tarde usadas como herramientas por los usuarios. Como propietaria de la plataforma PaaS, la empresa es responsable de los datos y las aplicaciones que contiene, pero no del almacenamiento, la red, los servidores o el sistema operativo.

Autoevaluación

Identifica si las siguientes frases son verdaderas o falsas

Los entornos de nube son la solución ideal a nivel forense

○ Verdadero ○ Falso

Falso

Los sistemas en nube son una gran solución para las empresas pero a nivel forense pueden suponer varios problemas tanto de extracción de evidencias como de validez y legalidad de las mismas.

La nube privada se considera la mejor solución pero tambien la más costosa.

○ Verdadero ○ Falso

Verdadero

Es la solución que mejor nos permite tener control sobre los datos pero por contra requiere más inversión.

Una nube hibrida combina lo mejor de ambos mundos, proporcionando una solución para los datos sensibles y un coste menor para datos que no se necesitan tener en una nube privada o en local.

○ Verdadero ○ Falso

Verdadero

Se considera la solución intermedia que aporta control de datos y ahorro de costes.

Los temas regulatorios no influyen a nivel técnico dentro del análisis forenses en entornos de cloud

○ Verdadero ○ Falso

Falso

Regulaciones como GDPR o ley Patriot condiciona los procesos y la validez de las evidencias extraídas de la nube.

1.3.- Estrategias y fases del análisis forense en Cloud.

Pexels (Dominio público)

Como comentábamos al principio del curso, dentro del análisis forense digital uno de los objetivos es que todo nuestro trabaje sea verificable, auditable y reproducible ya que cualquier evidencia que se encuentre o conclusión del informe debe ser admisible en un tribunal de justicia dentro de la jurisdicción correspondiente. En un forense tradicional la mayoría de las veces, las pruebas encontradas pertenecen al propietario de la tecnología, lo que facilita obtener el permiso para usar estas pruebas en el caso.

El análisis forense en la nube hace que esta búsqueda de pruebas sea un poco más compleja. Si bien el investigador sigue los mismos métodos en el análisis forense en la nube que en el análisis forense digital tradicional, las líneas pueden desdibujarse sobre quién posee la evidencia y dónde es admisible en la corte. La principal fase que cambia es la de la adquisición, no tanto a nivel técnico sino mas bien a nivel logístico y legal.

Con los servicios basados en la nube, los datos pueden almacenarse fuera del sitio en varias ubicaciones o en un servidor propiedad de un tercero. Por ejemplo podemos tener una máquina comprometida de un servicio que nos da una empresa china, que está en la nube de Microsoft en Alemania (es decir empresa americana pero el servidor físico en Unión

Europea).

A nivel de metodología y fases seguiremos los mismos principios que hemos visto durante el curso, pero durante la fase de identificación si hay alguna evidencia en la nube deberemos anotar tipo de servicio, proveedor y legislación vigente según donde esté la evidencia.

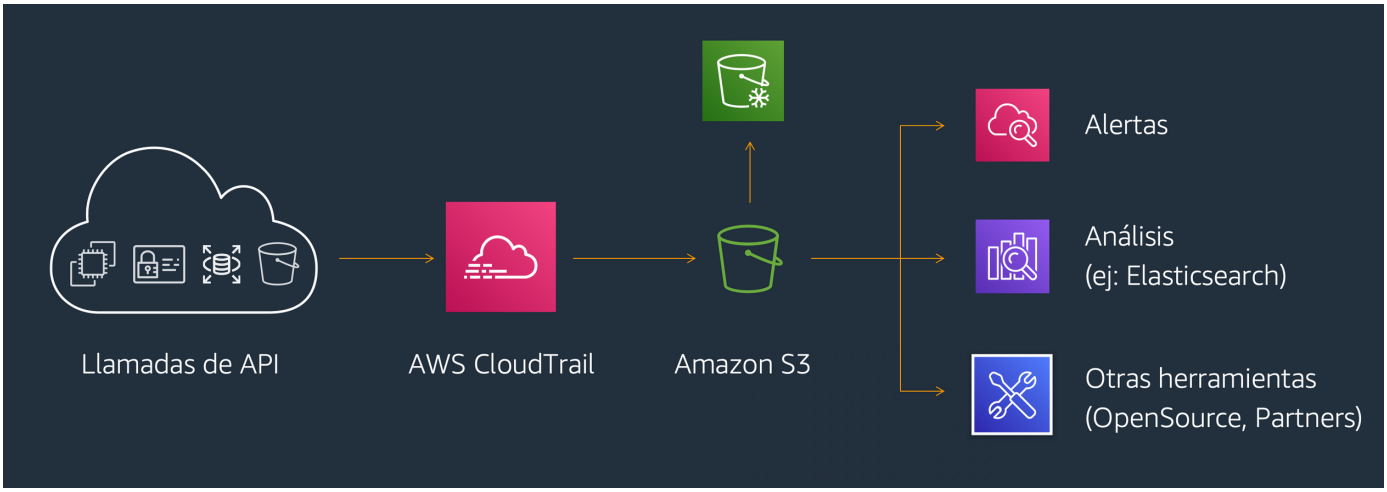
En la fase de extracción tenemos que garantizar que podemos acceder a la evidencia, conseguir los permisos necesarios, garantizar que será valida en juicio y que estamos cumpliendo con todas las normativas vigentes.

Debes conocer

Repercusión Legal

El objetivo principal de securizar los datos del dispositivo móvil es prevenir la fuga de información del dispositivo.

1.4.- Utilizar herramientas de análisis en Cloud.



Amazon (Captura de pantalla)

Dentro de las herramientas disponibles para realizar análisis forenses tenemos varias alternativas:

- Cellebrite UFED Cloud Analyzer
- Cloud Trail (Para entornos de Amazon)
- Frost
- OWADE
- Belkasoft X (cloud)

Desde el punto de vista de herramientas, tenemos dos categorías, herramientas:

- Herramientas forenses puras
  - Nos permiten como principal característica tener conectores para los principales servicios de cloud, independientemente del servicio que tengamos contratado (PaaS, IaaS, etc) de tal manera que podamos de forma sencilla realizar forenses o extracciones.
- Herramientas Cloud
  - Son herramientas enfocados al acceso a datos de cloud que podemos usar a nivel forense.

Port ejemplo tenemos AWS Cloud Trail que no solamente nos permiten hacer las extracciones necesarias dentro de un forense sino que además nos permiten tener telemetría de nuestros datos, saber cómo se acceden, desde dónde etc.

Los principales beneficios de este tipo de herramientas:

- **Simplificar el proceso de cumplir con las normas internas de las políticas y estándares regulatorios.**
- **Acceder de forma sencilla a múltiples proveedores de cloud sin importar el tipo de servicio.**
- **Detección de casos de acceso no autorizados.**
- **Alertas en tiempo real que podemos integrar en nuestro entorno.**
- **Disponer de un entorno de búsqueda dónde poder revisar cualquier dato que tengamos en el cloud.**