CAI-4. PROTOCOLOS DE CORREO SEGURO Y ESTEGANOANÁLISIS

CONFIDENCIAL

En esta sesión de trabajo el cliente es una **empresa farmacéutica** que se dedica a la investigación, desarrollo, fabricación y comercialización de productos para terapias avanzadas centradas en el tratamiento de la reumatología, gastroenterología, oncología, virología, trastornos neurológicos y otras afecciones metabólicas críticas, nos consulta sobre su intención de mejorar la seguridad de las comunicaciones por correo entre los directivos del consejos de administración de la empresa y para la comunicaciones con los Directores de los diferentes departamentos (financiero, investigación, producción,…) que tiene la empresa. **Para ello dicha empresa nos solicita la formación en temas de ciberseguridad, junto con la investigación forense sobre correos de ciertos empleados de la empresa.**

Los directivos nos plantean en esta consultoría tres preocupaciones concretas:

- **Procesos de envío de correo seguros** usando criptografía
- **Procesos de investigación forense digital sobre correos electrónicos recibidos que son falsos (phishing y spear phishing)**
- **Procesos de investigación forense digital sobre correos electrónicos envíados por cierto personal de la empresa y que podrían estar produciendo fuga de información empresarial (exfiltración de información confidencial)**

Son conscientes en la empresa que la Constitución española protege la confidencialidad del correo personal. Pero hay que tener en cuenta el **empleador puede inspeccionar los correos y demás comunicaciones electrónicas de sus asalariados**, ya sean profesionales o privadas con ciertas limitaciones, según sentencia del 12 de Enero de 2016 de**l Tribunal Europeo de Derechos Humanos de Estrasburgo,** en la que indica que se encuentra dentro de la ley que una empresa revise los correos electrónicos de su plantilla. El fallo, referido a un caso ocurrido en Rumanía, **incluye los mensajes enviados desde el correo corporativo (en horario laboral) y los que se transmitan a través de cuentas privadas, pero operadas desde el ordenador del trabajo.** El derecho español establece que **el trabajador tiene que ser notificado antes de que se le monitorice su ordenador en la empresa.**

Por todo ello las consultas que nos presenta esta entidad farmacéutica son las siguientes:

Consulta 4.1. CONFIDENCIALIDAD EN LA TRANSMISIÓN DE INFORMACIÓN MEDIANTE EL PROTOCOLO PGP

Contexto: Los directivos desean enviar correos que contienen información muy sensible de forma segura y con posibilidad de firmarlos usando para todo ello **seguridad end-to-end** mediante criptografía.

Consulta: En esta consulta nos solicita la empresa que se **atienda a las siguientes consultas:**

- **Realizar un pequeño tutorial sobre el proceso para configurar los directivos de la empresa el cliente de correo** (los más comunes Thunderbird, Outlook, etc.) o bien cómo se realiza tal configuración a través de las diferentes aplicaciones Web para envío de correo seguro/firmado y el proceso cómo se realiza el envío/recepción de correos **seguros** usando PGP **y el firmado del contenido de estos.**
- Mostrarles a los directivos los mecanismos que se usan para **que las claves usadas en el envío y firmado se guarden en las aplicaciones correspondientes de forma segura y por lo tanto las personas no autorizadas no pueden acceder a ellas**
- Mostrarles a los directivos **cómo pueden disponer de los certificados de revocación de las claves usadas por si hay en alguna ocasión el robo de alguna de ellas.** Por lo que

también **nos solicita un tutorial sobre cómo se genera dicho certificado y cómo se podría usar en caso de robo de la clave para revocar dicha clave.**

Consulta 4.2. DETECCIÓN E IDENTIFICACIÓN DE CORREOS FALSOS (PHISHING Y SPEAR PHISHING)

Contexto: Los directivos de la empresa reciben muchas veces correos falsos, y que se encuentran personalizados para facilitar el engaño (spear phishing) y desean que le ayudemos a conocer cómo podrían identificar éstos de los realmente legítimos, pues muchas veces ya se han usado con ellos el spear phishing y realmente son bastante difícil identificarlos.

Consulta: En esta consulta **los directivos de la empresa cliente nos solicitan un pequeño tutorial sobre que tendría que tenerse en cuenta** para determinar usando tanto el ***payload*** como las cabeceras del correo la falsedad o no del mismo, por todo ello nos solicitan:

- **Pequeño tutorial sobre el proceso para comprobar la falsedad o no de los correos atendiendo a las características que considera TopTen** y que deben comprobarse de forma lo más automática posible (usando herramientas informáticas).
- Mostrar la e**jecución del proceso que se llevaría a cabo en dos correos que podrían ser phishing o spear phishing** (debe el Security Team preservar la confidencialidad de los mismos).
- Mostrar al cliente **cómo las beacons o bitácoras de los correo electrónicos pueden exfiltran información empresarial y cómo se podría evitar técnicamente** dicha exfiltración.

Consulta 4.3. DETECCIÓN E IDENTIFICACIÓN DE CORREOS ENVIADOS POR EMPLEADOS QUE PUEDE SUPONER LA FUGA DE INFORMACIÓN EMPRESARIAL.

Contexto: Se ha presentado a los directivos de la empresa farmacéutica una denuncia del **Responsable del Departamento de Investigación contra varios empleados de la entidad** por considerar que están enviando información confidencial de la misma a terceras personas ajenas a la entidad farmacéutica de forma codificada utilizando quizás algún método relacionado con la esteganografía digital.

Consulta: Nos solicita el cliente a los ingenieros/as de INSEGUS que actuemos como perito digital forense, contando con las evidencias digitales que son un conjunto de imágenes enviadas sobre la que se cree existe información confidencial oculta. Se adjunta en este documento dichas imágenes para llevar a cabo el estegoanálisis. El cliente con esta información nos requiere:

- **Especificar el proceso para detectar e identificar las Imágenes que contienen mensajes ocultos** usando esteganografía digital.
- **Presentar claramente en el informe si considera que existe una fuga de información o no en dichas imágenes, justificando adecuadamente la respuesta.** Si existe alguna imagen o imágenes que contengan información confidencial de la empresa se debe realizar el envío por correo seguro a gasca@us.es indicando el contenido de dicha información confidencial.
- Se sospecha por la empresa, que la información confidencial textual en la imagen puede no ir íntegra por haber sido sometida a transformaciones, pero con las correspondientes transformaciones por la persona que lo recibe podría obtenerse la información confidencial que se desea transmitir. El cliente nos solicita que mediante al menos tres pruebas le mostremos si ello es posible o no. Por favor, **presentar dichas pruebas**. Muchas gracias.

Consejos:

- **Revisar el Tema 4 en el que** se tratan todos los temas relacionados con las anteriores consultas.

- Revisar el documento que se ha incluido en esta consultoría sobre las ***Características a considerar para detectar los correos de phishing o spear phishing***
- Revisar la Guía de elaboración y evaluación de los CAI.
- Tener en cuenta **los check del ciclo de mejora continua que se han publicado para los anteriores CAI**
- No copiar contenido de **esta especificación en el informe solo apoyar la respuesta con el contenido de este.**
- No copiar contenido de herramientas de consulta o de IA generativa en el informe (En el caso que la **herramienta anti-plagio encuentre un grado mayor del 30% con respecto al texto ya publicado por otras personas o artefactos de IA generativa, se valorará toda el CAI con grado de satisfacción nulo.)**