CAI 5. CONSULTA SOBRE LA SEGURIDAD DE LOS CORREOS PARA DIRECTIVOS DEL CONSEJO DE ADMINISTRACIÓN DE EMPRESA FARMACÉUTICA

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 la empresa nos solicita la formación en temas de estos temas de ciberseguridad, junto con la investigación forense sobre correos de empleados de la empresa.**

Los directivos nos plantean en esta consultoría dos aspectos de formación:

- **Procesos de envío de correo seguros** usando criptografía y esteganografía
- **Procesos de investigación Forense digital sobre correos electrónicos falsos o que podrían estar produciendo fuga de información empresarial**

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 del **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 el cliente nos solicita la respuesta técnica a las siguientes consultas para la formación del personal correspondiente:

Consulta 5.1 Proceso de envío de correos seguros y/o firmados por los directivos usando criptografía

Los directivos desean enviar correos seguros y con posibilidad de firmarlos usando **seguridad end-to-end mediante critpografía.**

Una de las posibles soluciones tecnológicas para enviar correo seguro y firmado sería ***la instalación de PGP en un cliente de correo*****,** el Equipo Consultor podría escoger cualquier otra opción pues el cliente no ha requerido un sistema concreto. **PGP** junto con **S/MIME** son los protocolos más utilizados para conseguir privacidad y autenticación en los mensajes de correo electrónico. A ello ha contribuido su distribución como herramientas gratuitas, así como su puesta

al día en sucesivas versiones mejorando sus capacidades. PGP se puede encontrar como plug-in para la mayoría de clientes de correo electrónico, incluyendo Exchange y Outlook de Microsoft, Eudora o Pine, Thunderbird, ...

PGP nos permite:

- **Cifrar mensajes y archivos** para que no resulten legibles sin nuestra autorización (Confidencialidad).
- **Firmarlos digitalmente para asegurarnos que no son modificados sin nuestro consentimiento y que demuestra nuestra identidad al destinatario.** (Integridad y autenticación).

En esta consulta nos solicita la empresa farmacéutica que se aborden los siguientes aspectos:

1. **Pequeño tutorial sobre el proceso para configurar los directivos de la empresa el cliente de correo y el proceso cómo se realiza el envío/recepción de correos.**
2. **Envío por cada uno de los componentes del Security Team de INSEGUS** de un **correo cifrado y firmado con la presentación de la consultoría a la dirección de correo de la persona que os ha encargado en INSEGUS la consultoría (gasca@us.es)**.

Valoración de la consulta será el 25% y dependerá significativamente de la calidad técnica de detalle que presente el *Security Team* consultor en sus respuestas/envíos

Consulta 5.2 Análisis de herramientas para el envío de correos/mensajes seguros por los directivos usando esteganografía

La **esteganografía digital** es una técnica que consiste en la ocultación de la información sobre un estego objeto (imagen, sonido, video, …) donde se cubrirá la misma y el **estegoanálisis** es detectar aquella información que se oculta.

Muchas herramientas implementan la esteganografía. Generalmente implementan una sola técnica, la más común es ***Least Significant Bit (LSB).*** Pero los datos pueden también ocultarse con otros métodos más avanzados, tales como la técnica ***Karhunen-Loeve Transform*** (KLT), por el algoritmo ***F5***, que usa una transformación DCT en ficheros JPEG, etc... También existen herramientas visuales que permiten el uso de la esteganografía/estaganálisis, basándose en el paradigma de procesos de negocio, tal como ***Visual Steganographic Laboratory.***

Igualmente encontramos **aplicaciones para estegoanálisis**, tales como el ***RS-Analysis***: que es un método eficiente de estegoanálisis para los métodos LSB, ***Binary Similarity Measures (BSM)*** que usa clasificadores relacionados con las Máquinas de Soporte Vectorial (SVM) que puede usarse para cualquier clase de esteganografía digital, etc…

La entidad farmacéutica nos comunica que se puede usar cualquier herramienta que considere oportuna el equipo Consultor para el estudio, ellos han estado pensando en adoptar la herramienta ***Steghide*** que soporta un número razonable de formatos de ficheros contenedores: JPEG, BMP, WAV y AU. Para los dispositivos Android de los directivos nos comunican que están considerando en la entidad el uso de la herramienta ***Steganography Master***, que puede codificar la información enviada. El mensaje podrá ser leído por ellos siempre que tengan la misma app, y se pueden asegurar proporcionando el correspondiente password entre ellos. Y para dispositivo iOS están considerando otra muy similar llamada ***Steganographia***, y que también utiliza fotografías y todo tipo de imágenes para ocultar los textos de los mensajes que se desean enviar.

Se nos solicita por el cliente en esta consulta:

1. **Análisis de herramientas de esteganografía de imágenes o voz o video y seleccionar al menos 3 herramientas para que desde un dispositivo de sobremesa** se puedan enviar correos/mensajes usando esteganografía digital adjuntando la imagen/voz/video con el correspondiente mensaje embebido,
2. **Analizar herramientas de esteganografía de imágenes o voz o video al menos 3 herramientas para que desde dispositivos móviles se puedan enviar correos o mensajes usando esteganografía digital adjuntando** la imagen/voz/video con el correspondiente mensaje embebido,

Tanto para el punto uno como el dos los directivos nos han comunicado que los criterios que debe seguir el Equipo Consultor para seleccionar de las 2 herramientas de cada apartado deben estar relacionadas con la **Alta Capacidad de Almacenamiento, Alta Confidencialidad, Usabilidad y Robustez a distorsiones/escalado/compresión/recorte de las imágenes (evitando la pérdida de la integridad de la información transmitida), tiempo de ocultación y recuperación del mensaje bajo).** Los directivos necesitarían conocer todos los detalles del análisis realizado y las bondades/inconvenientes de cada una de las herramientas y las configuraciones más adecuadas para sus dispositivos de trabajo.

3. Se requiere el envío de un correo de un mensaje por cada miembro del Equipo Consultor conteniendo el siguiente texto:

   Debido a la gran potencia anticoronavirus en las pruebas que hemos realizado en nuestro laboratorio vamos a proceder a fabricar en la empresa el producto Remdesivir

   a la dirección de correo de la persona que os ha encargado en INSEGUS la consultoría (gasca@us.es). Tenga en cuenta que el destinatario, en el caso que añadieran una clave cuando realizan la esteganografía, tendría que conocer dicha clave por algún medio seguro. Por ello en el informe se debe reflejar esto como se haría por el destinatario.

Valoración de la consulta será el 25% y dependerá significativamente de la calidad técnica que presente el Ingeniero/a Consultor en sus respuestas/envíos

Consulta 5.3 Procesos forense digital para identificar correos falsos, enlaces y adjuntos maliciosos

Los directivos de la empresa reciben muchas veces correos falsos y desean que le ayudemos a conocer cómo podrían identificar éstos de los realmente verdaderos, pues muchas veces han usado con ellos el ***spear phishing***. Por ello nos han indicado que en esta consulta desean:

1. Pequeño tutorial sobre el proceso forense digital que tendría que seguir para determinar usando tanto el ***payload*** como las cabeceras del correo la falsedad o no del mismo.
2. Pequeño tutorial sobre el proceso para comprobar la falsedad o no de los posibles links que se incluyen en los correos
3. **Pequeño tutorial sobre el proceso forense digital para determinar si los adjuntos que se añaden a los correos pueden resultar maliciosos** para el negocio o no**.**
4. **Aplicar dichos procesos para un caso concreto de un correo falso** que disponga el Security Team (si no dispusiera de alguno, la empresa INSEGUS podría proporcionar uno bajo petición) y presente en el informe todos los pasos que se han seguido de acuerdo a lo indicando en los anteriores puntos.

Valoración de la consulta será el 25% y dependerá significativamente de la calidad técnica que presente el Ingeniero/a Consultor en sus respuestas/envíos

Consulta 5.4 Proceso forense digital para identificar correos que pueden implicar fuga de información empresarial

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. 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 quiere determinar:

1. Imágenes que contienen mensajes ocultos y proceso/técnica usada para la determinación de si se está usando esteganografía digital.
2. Imágenes que se están compartiendo información confidencial de dicha entidad farmacéutica. **Presentar claramente en el informe si considera que existe una fuga de información o no en dichas imágenes, justificando adecuadamente la respuesta.** Para el análisis de la imagen el perito forense puede utilizar cualquier herramienta que estime oportuna.

Valoración de la consulta será el 25% y dependerá significativamente de la calidad técnica que presente el Ingeniero/a Consultor en sus respuestas/envíos

Las respuestas a todas estas consultas **se incluirán en el Informe Ejecutivo de la Consultoría.**

El presupuesto acordado con el cliente para esta consultoría ha sido de **1835€ + IVA**.

Normas del entregable

- El plazo de entrega de dicha consultoría finaliza el **día 5 de Mayo de 2020 a las 10:30 horas.**
- Se debe realizar la entrega al CISO por parte del ingeniero ***Consultor Jefe*** a través de la Plataforma de Enseñanza Virtual un **archivo *STnumCAI5.pdf*** que contenga las respuestas a las consultas realizadas, además no olvide que se deben enviar por parte **de todos los componentes del Security Team dos correos electrónicos(uno con criptografía y otro con esteganografía) a gasca@us.e**s. (No se debe indicar en los documentos los ingenieros/as que han participado en el Equipo de Trabajo Consultor, **pero si en el mensaje enviado**).