Términos de Referencia para la contratación de una Auditoría en términos de Ciberseguridad.

NECESIDADES

Médicos del Mundo España (en adelante MdM) ha detectado la necesidad de contratar los servicios de una Auditoría en términos de Ciberseguridad.

Esto es así, ya que en los últimos años tanto la infraestructura tecnológica como el volumen de usuarios y dispositivos ha aumentado sustancialmente debido al crecimiento de la organización.

El objetivo principal del proyecto propuesto es el de **realizar una evaluación objetiva, neutral y actualizada del estado de seguridad** de la plataforma informática de Médicos del Mundo y todos sus dispositivos, desde el punto de vista de la seguridad de la información contenida en dicha plataforma, con una visión proactiva, que permita anticiparse a problemas futuros y con el mínimo impacto posible en la infraestructura.

El proyecto de auditorías de seguridad y hacking-ético deberá satisfacer las necesidades de la organización de medir la seguridad en los sistemas a analizar.

El objetivo general de esta consultoría debería englobar los siguientes aspectos:

DESCRIPCION DE SERVICIOS

Auditoría. Permite entender las necesidades del cliente en materia de seguridad y sistemas. El objetivo es conocer la realidad del negocio del cliente e identificar su foco de riesgo.

Planes de acción. Con la información que extraemos en la fase de auditoría se diseñan los planes de acción, estableciendo una hoja de ruta en la que acompañamos al cliente. Se priorizan los proyectos que pudieran identificarse y se cuantifican las inversiones.

Mecanismos de defensa. Se establece una planificación de los proyectos que permitirá mejorar el nivel de seguridad de la compañía.

Monitorización del servicio como aspecto clave de la seguridad. Necesidad de monitorizar de forma constante y proactiva que está ocurriendo en nuestros sistemas

IDENTIFICACIÓN DE RIESGOS

Durante el **diagnóstico de ciberseguridad** se llevarán a cabo las siguientes tareas:

Recopilación de información: El equipo de seguridad obtendrá el mayor número de información sobre los sistemas, dispositivos, la organización y sus usuarios a través de herramientas automatizadas, consultas a motores de búsquedas y pruebas manuales.

Identificación de Servicios: Una vez establecida la lista de activos a auditar, tanto los ofrecidos por el cliente como los nuevos descubiertos se procederá a identificar los servicios ofrecidos por los mismos. (Incluyendo redes Wifi corporativas y NO corporativas)

Consideraciones sobre el puesto de trabajo: Hay que tener en cuenta que existen usuarios que trabajan tanto en oficinas como en remoto, por lo que es necesario evaluar este aspecto, así como el uso de dispositivos móviles.

Análisis de vulnerabilidades: Una vez se han identificado todos los servicios junto con sus versiones, se procede a la búsqueda de posibles vulnerabilidades en las versiones de los servicios localizados.

Explotación de vulnerabilidades: cuando ya tenemos localizadas todas las vulnerabilidades procedemos a su explotación para evitar de que se traten falsos positivos o por el contrario se pueda obtener información sensible tras su explotación.

Post explotación: Una vez las vulnerabilidades ha sido explotada lo que se trata es de poder realizar diversas técnicas que comprometan la seguridad de la entidad, como obtener el usuario administrador, tener privilegios en el dominio, etc.

Una vez finalizada la fase de **explotación** comenzaremos con la elaboración del **informe** en el que se documentará las vulnerabilidades y las recomendaciones que permitirán elevar el nivel de seguridad perimetral e interno del cliente.

ANÁLISIS

Análisis de resultados: El equipo de seguridad encargado de realizar el hacking ético analizará la información obtenida con el objetivo de identificar el impacto que esta puede suponer para la entidad.

Análisis de impacto: en esta fase se mide el posible riesgo al cual se está expuesto, determinando el impacto de la explotación de las vulnerabilidades y su probabilidad de ser atacado por esos vectores de entrada, los cuales supondría los siguientes riesgos:

- **Riesgo de perdidas:** referente a la posible fuga o robo de información.
- **Riesgo en los procesos:** debido a posibles ataques de denegación de servicio.
- **Riesgo técnico:** presencia de vulnerabilidades en los activos.
- **Riesgo Organizativo:** a modo de métrica del nivel de riesgo global.

La finalidad del diagnóstico es poner a prueba la capacidad de detección/resistencia de la organización ante un ataque externo. Por cada una de las vulnerabilidades encontradas durante el análisis de hacking ético.

ACCIONES

Mejoras inmediatas: un atacante puede hacerse con el control del sistema o puede obtener información altamente sensible. Las vulnerabilidades de este nivel pueden incluir el acceso completo de lectura de archivos, potenciales puertas traseras o listas de usuarios y contraseñas.

Mejoras a corto plazo: el atacante puede obtener información específica almacenada en el activo, incluyendo la configuración de seguridad. Las vulnerabilidades de este nivel pueden incluir la divulgación parcial del contenido de los archivos, el acceso a ciertos archivos en el equipo, la explotación de directorios, ataques de denegación de servicio o el uso no autorizado de servicios.

Mejoras a medio plazo: el atacante puede obtener información del activo, como la versión exacta del software instalado. Con esta información un atacante puede explorar fácilmente vulnerabilidades conocidas específicas para la versión localizada.

Mejoras a largo plazo: presencia de vulnerabilidades o problemas que puedan degradar considerablemente la seguridad a largo plazo.

ENTREGABLES

A la finalización del proyecto se entregará a Médicos del Mundo la siguiente documentación:

● **Informe técnico de auditoría:** Documento donde se expondrán de forma detallada cada una de las vulnerabilidades detectadas clasificándolas en función de distintos parámetros: criticidad, impacto, tipo, servicio afectado, nivel de riesgo técnico y ejecutivo, descripción y recomendación para su mitigación. Este informe estará acompañado de métricas de riesgo técnico y ejecutivo, así como de categorización de vulnerabilidades.

● **Plan de remediación:** Hoja de ruta, que será proporcionada a Médicos del Mundo, con el objetivo de facilitar la clarificar las medidas técnicas a tomar por los departamentos involucrados en la corrección de las vulnerabilidades o debilidades detectadas.

PROPUESTA TÉCNICA Y ECONÓMICA

La propuesta técnica contendrá:
- Solución (o soluciones) propuesta(s)
- Cobertura en los aspectos indicados anteriormente.
- Una propuesta de proyecto en Fases.
- Equipo de trabajo.
- Experiencia de la organización en trabajos similares y referencias.
- Fecha tentativa de inicio y plazos estimados de ejecución del proyecto.

La propuesta económica contendrá:
- Coste de cada solución propuesta.
- Desglose de los costes por cada concepto o cada fase definida.