**Caso de Estudio 2 – Canales Seguros Logística y Seguridad Aeroportuaria**

1. [20%] Análisis y Entendimiento del Problema.
2. Identifique los datos que deben ser protegidos por la aplicación Novasoft financiero en línea. Justifique su respuesta (para cada dato responda la pregunta ¿Si un actor no autorizado consigue acceso al dato mencionado, ¿cómo podría afectar la empresa?
   1. **Instalación de Malware**

Si aparece un actor no deseado, podría instalar programas maliciosos que podrían provocar daños importantes en el sistema. En caso de que sea un malware, se podrían tener varias consecuencias. La intrusión de un gusano en el sistema puede provocar un gran tráfico en el sistema o en la red y pueden ser saturados, ya que el objetivo de un gusano es replicarse al máximo. Dado que estamos hablando del servidor que administra las transacciones financieras, esto representaría grandes pérdidas para la empresa. También, en el caso de que los gusanos tengan un *payload*, se podrían dañar los datos del sistema, de la computadora o de la red. Además, si estos *payload* instalan una puerta trasera, es probable que traigan otro malware para que controle la computadora. Como resultado, los sistemas de la empresa colapsarían, lo que afectaría los datos de transacción, las facturas y el funcionamiento de los sistemas de la oficina central directamente. En consecuencia, se formaría un desastre financiero para la empresa, desde servidores de saturación hasta la destrucción del sistema. Adicionalmente, este problema causaría una disminución y afectación en la imagen de la compañía y, por lo tanto, una disminución en la asistencia a su servicio.

* 1. **Modificación de datos**

Si un actor externo modificaría los datos presentes en la aplicación en línea de Novasoft financiero, esto podría llevar a situaciones difíciles para la compañía. Por ejemplo, al eliminar las cuentas de los clientes que tendrían una deuda con la empresa, lo que podría resultar en una pérdida financiera, o modificarla, lo que podría generar situaciones complicadas entre el cliente y la empresa y podría dañar su imagen. La imagen de una compañía es primordial, especialmente en el ámbito de la seguridad, daría como resultado una disminución de clientes, y por lo tanto no solo una pérdida de dinero sino también un peligro para los clientes que ya no pueden protegerse contra actos de interferencia ilícita en la aviación civil. Además, al cambiar el efectivo, se perderían las cuentas de la empresa. Además, por la modificación de los datos, podemos hablar de creación, cómo podría ser la creación de Puertas Traseras y enviar sumas de dinero no detectables por el sistema a terceras cuentas bancarias, que luego se convierten en grandes sumas de dinero.

* 1. **Robo de datos**

Los dos últimos puntos llevan a este. De hecho, un actor no deseado podría robar datos confidenciales de la compañía que podrían debilitar el negocio. Esta información puede ser robada por un caballo de Troya, por ejemplo. El usuario sería redirigido a un servidor fraudulento y, cuando deba identificarse con su nombre de usuario y contraseña, será robado por la persona con acceso directo al servidor fraudulento. El ladrón tendrá acceso a todos los datos existentes, y ningún otro dato del sistema será confidencial. Fotos, informes para los distintos clientes en curso, datos bancarios, efectivo ... Tanta posibilidad de que sea mucho peor que borrarlos. Como resultado, el actor podría vender los datos a los competidores, o rescatar a Novasoft sin la certeza de que los datos nunca se utilizarán indebidamente. Esto afectaría grandemente el negocio y el sistema.

* 1. **Usurpación de identidad (Spoofing)**

Si el actor por los métodos anteriores logra robar la contraseña, entonces puede tomar la identidad de éste. Luego, puede reclamar ser ese empleado y falsificar información diversa sobre él, pero también otras informaciones de otras personas según la identidad de la persona que fue usurpada. Esto podría causar un verdadero problema dentro de la empresa, especialmente si la persona en cuestión es una persona con responsabilidades. Podría enviar información fraudulenta a otros empleados y / o tener información confidencial. Luego, podría propagar este robo de identidad a otras personas de la empresa redirigiéndolos a técnicas que se hayan visto anteriormente, como el Caballo de Troya. También podría causar conflictos dentro de la empresa.

1. Identifique cuatro vulnerabilidades del sistema, teniendo en cuenta únicamente aspectos técnicos (no organizacionales o de procesos). Identifique vulnerabilidades no solo en lo relacionado con la comunicación sino también con el almacenamiento. Explique su respuesta en cada caso.
2. [10%] Propuesta de Soluciones.
3. Para cada una de las vulnerabilidades que usted identificó en el punto anterior, proponga mecanismos de resolución/mitigación. Justifique brevemente por qué el mecanismo propuesto resuelve la vulnerabilidad. En sus justificaciones tenga en cuenta aspectos relacionados con eficacia, costo, eficiencia, flexibilidad, aspectos de implementación, y otros aspectos técnicos que considere convenientes.