**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 modifica los datos presentes en la aplicación en línea de Novasoft financiero se podría convertir en un gran problema y generar situaciones complicadas para la compañía. Por ejemplo, al eliminar las cuentas de los clientes que tendrían una gran deuda con la empresa, se podría generar una pérdida financiera. Adicionalmente, esta situación puede generar inconvenientes y situaciones tensas entre el cliente y la empresa, y deteriorar la imagen de la empresa. La imagen de una compañía es primordial, especialmente en el ámbito de la seguridad, y si esta se deteriora se tendría como resultado una disminución de clientes y una pérdida de dinero. También, los actores externos que tengan acceso a los datos pueden hacer modificaciones a la información a su conveniencia que ponen en riesgo la integridad de estos.

* 1. **Robo de datos**

Un actor no deseado podría robar datos confidenciales de la compañía que pondrían en duda la seguridad del sistema de la compañía y utilizar dicha información para hacer cualquier tipo de acto ilegal. Por ejemplo, un usuario común del sistema puede ser 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. Informes, bases de datos, estados financieros, datos bancarios, transacciones, entre otros. Como resultado, el actor podría vender los datos a los competidores, o simplemente exponerlos sin la certeza de que los datos se utilizarán indebidamente o no.

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

Si el actor por los métodos anteriores logra robar la contraseña y tener acceso al sistema como un empleado, entonces puede tomar la identidad de éste y luego reclamar ser ese empleado y falsificar información diversa sobre él. Además, el actor maligno no solo tendría información del empleado a el cual está suplantando sino también a información de otros empleados, directivos y clientes dependiendo los permisos autorización que tenga el empleado que fue suplantado. Esto podría causar un verdadero problema dentro de la empresa, especialmente si la persona en cuestión es una persona con responsabilidades importantes. Todos estos problemas que causa la suplantación de identidad deben ser prevenidos y manejados por el mismo sistema para que se compruebe que la persona que está ejerciendo dichas acciones realmente es el individuo verdadero y no un actor externo suplantándolo. En resumen, las vulnerabilidades que tenga un sistema que faciliten la suplantación por agentes externos puede ser caótica dentro de un sistema financiero en línea como el de Novasoft. Ya que, constantemente se están realizando registros de transacciones y se está manejando información muy importante, y por lo tanto es de suma importancia que el sistema prevenga y maneje este tipo de vulnerabilidades.

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.