Universidad de los Andes
Ingeniería de Sistemas y Computación
ISIS 2203 Infraestructura Computacional
Francisco José MacAllister 201533772
Laura Maya 201423854

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

**A. [20%] Análisis y Entendimiento del Problema.**

Puntos 1 y 2:
El primer factor importante encontrado fue la posible modificación o lectura de valores confidenciales. Si un actor no autorizado consigue acceso (modificación o lectura) de los valores podría causar grandes daños, incluso irreparables tanto en la contabilidad como en la confianza que los clientes depositan en la compañía. En el caso de los clientes, un actor no autorizado puede obtener no solo la información privada de los clientes (Nombre, dirección, historial, etc) sino que además podría consultar los estados financieros de dicha persona (dimensiones de compras y números de tarjetas y cuentas). El robo de la información financiera podría fácilmente causar enormes estafas al utilizar suplantación de identidad (más aun cuando se posee información adicional de la identidad del dueño de la tarjeta) lo que causaría una caída en la confianza de la compañía significativa. Perder la confianza fácilmente podría llevar a la quiebra, además de las inmensas multas y demandas que se podrían tomar en contra de NovaSoft. Lo segundo, serian valores internos de la compañía como asignación de presupuestos, saldos y contratos entre clientes y la compañía. La modificación de estos valores podría causar grandes inconvenientes internos si no son encontrados de manera oportuna, causando faltas de presupuesto, o exceso de presupuesto (que sea gastado) así como falta en los compromisos con los clientes.

Tanto la suplantación de identidad para el robo de datos confidenciales como la modificación de valores confidenciales internos de manera masiva podría causar un inconveniente grave si no se detecta a tiempo, sin embargo, estos ataques masivos pueden ser hallados de manera oportuna debido a las posibles alertas que pueden existir. Existe un problema que puede llegar a ser inclusive más grave que el mencionado anteriormente. Es posible que un actor no autorizado logre instalar un programa para lograr esta manipulación de manera continua pero silenciosa (virus). Al mantener un acceso constante a los datos se podría conseguir realizar todo lo anterior, pero con pocos datos a la vez, así que descubrir un ataque podría resultar mas difícil, por lo que se podría pasar desapercibido un mayor tiempo. Esto igualmente causaría una disminución significativa para la empresa, causando una disminución de los clientes por las razones antes mencionadas. Aun cuando el software no necesariamente modifique algún dato, es posible que exista únicamente para realizar espionaje en los medios de transmisión de la aplicación. Esto permitiría ver al instalador todas las transacciones realizadas en todo momento, y esta última operación sería la más difícil de rastrear, pues al no realizar ninguna modificación a los datos no existirían inconsistencias lógicas al momento de realizar una comparación entre la aplicación en línea y la que no se encuentra en línea.

Vulnerabilidades detalladas:

1. Acceso a datos confidenciales (Acceso no autorizado al sistema y Robo de información): Esta vulnerabilidad representa la amenaza del robo de información. Esta información puede ser desde reportes históricos confidenciales almacenados por la compañía para realizar pronósticos y previsiones hasta datos sobre las transacciones realizadas por la compañía con sus proveedores. Esto implicaría un acceso no autorizado al sistema y tendría las repercusiones graves mencionadas anteriormente.

2. Acceso a información financiera (Fraude y robo de información): Esta vulnerabilidad representa la amenaza del robo de información, más específicamente de los clientes. Ya que la compañía debe almacenar información confidencial sensible como lo son números de cuentas, números de tarjetas crédito, así como transacciones realizadas con tarjetas débito, existe la posibilidad de que en un ataque se realice un robo masivo de dicha información. Al obtener estos datos del almacenamiento de la compañía se podría vender esta información en la Deep Web, o inclusive en páginas conocidas por este tipo de actividad (inclusive redes sociales). Todas estas acciones tendrían repercusiones graves como las que se mencionaron anteriormente.

3. Acceso a información propia o de los clientes (Spoofing o suplantación): Con este acceso, es posible que los atacantes (hackers) realicen el robo masivo de identidades. Con esto, no se afectaría de manera directa a la empresa en principio, pues lo más factible es que se utilice dicha información para realizar suplantación de identidad. Así, existe la posibilidad de que se utilice información como el nombre, cedula, teléfono, celular etc. con el fin de realizar transacciones bancarias (diferentes a la red de NovaSoft) suplantación notaria, o muchas otras actividades simples que pueden corromper la identidad de una persona por medio de la suplantación. Ya que esta información se encuentra disponible en la base de datos de los usuarios, si se logra acceder a este almacenamiento realizar esta tarea seria simple. Todo esto tendría serias repercusiones para la compañía una vez se conozca la información de las "filtraciones de información" como se menciona anteriormente. Por otro lado, también seria posible que un actor logre copiar la identidad de una persona dentro de la entidad para así lograr acceder al contenido que el sistema le permitía ver o modificar a esta persona. Con esto, el Spoofing seria directamente en contra de Novasoft, y no suplantación virtual como la que se realizaría con la información de los clientes. A través de esta suplantación se podría obtener acceso a todas las operaciones (permitidas por el sistema al usuario que fue robado) que se describieron anteriormente.

4. Acceso no autorizado al sistema (Instalación de software malicioso): Con esto, es posible que el actor que logro acceder al sistema realice la instalación de posible virus o malware en el sistema. Con esto no solo se puede mantener un contacto directo y permanente con las bases de datos (tanto de usuarios como propias), sino que además se puede observar de manera continua las comunicaciones que realiza Novasoft con cualquier otro actor (sea un cliente, un proveedor o un empleado). Esta vulnerabilidad seria posiblemente la mas grave dado la cantidad de datos a la que es posible acceder después de esto. Las repercusiones de la ocurrencia de esto se serian graves como se evidenció anteriormente.

Nota: se realiza la suposición para todos los argumentos anteriores que el actor logra autenticarse como un usuario legitimo con métodos poco convencionales diferentes a los permitidos por la lógica de la aplicación y obtiene los permisos requeridos por la aplicación para acceder a la información confidencial.

**B. [10%] Propuesta de Soluciones.**

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.

1. Acceso a datos confidenciales (Acceso no autorizado al sistema y Robo de información):
   Para intentar evitar el robo de información por medio del acceso no autorizado al sistema, se podría realizar un cifrado completo de toda la información. Aunque esto no resuelve el problema, si realizara una demora significativa en el robo. Con esta demora implementada, se debería reportar una notificación continua de cualquier usuario que se encuentre mirando o modificando información. Al realizar un análisis se podría intentar determinar que existe una persona externa a la organización (por medio de un sistema de comunicación permanente cifrada entre el servidor y los usuarios). Al utilizar un sistema de cifrado simétrico, donde la llave entre cada usuario y el servidor principal se transmitiría de manera física (dentro de las instalaciones de la compañía), se podría identificar rápidamente la conexión que no se encuentre enviando información al servidor con una llave reconocida, por lo que se podría actuar rápido con el fin de eliminar la conexión o bloquear el sistema en caso de ser necesario. Finalmente, seria necesario realizar una inversión significativa en seguridad (tanto software anti-espía como desarrolladores para realizar mantenimiento y mejoras constantes) debido a la sensibilidad del contenido que se maneja en la aplicación.

2. Acceso a información financiera (Fraude y robo de información):
   Se debería implementar un sistema de seguridad en la información almacenada, ya sea por medio del cifrado de esta o por medio de la contratación de un sistema de seguridad en la nube donde se mantenga asegurada. Si se utiliza la primera solución se garantiza que, si se logra acede a los datos (archivo) no se puedan interpretar el contenido de este al requerir una llave de seguridad para su desencriptación y posteriormente su lectura. Si se utiliza la segunda opción, se contrataría a una empresa especializada en garantizar la seguridad de la información almacenada en la nube. Este tipo de empresas se dedica a prestar servicios enfocados en la seguridad de los datos desde el diseño de la infraestructura y están en constante mejoramiento. De esta forma problemas de autenticación y de control de acceso se están teniendo en cuenta en todo momento y se

garantizan como parte del servicio contratado, asegurando el trabajo de personal especializado en la seguridad de la información y en prevención de ataques. De esta forma la información almacenada siempre se encontrará protegida y se podrá garantizar el servicio a los usuarios. Al tener esta información manejada por un tercero, se puede asegurar a los clientes certificados reales de protección de la información, y en caso de que el sistema sea vulnerado, de alguna forma se puede intentar restaurar la confianza del cliente por medio de un cambio de empresa reconocida.

3. Acceso a información propia o de los clientes (Spoofing o suplantación):
   A nivel de la compañía, lo primero es asegurarse de que las contraseñas de acceso de todos los usuarios sean suficientemente robustas para que no sean fáciles de detectar por terceros y acompañado de esto, realizar capacitaciones sobre los riesgos que implica compartir esta información, de esta manera las personas sestaran mejor enteradas y estarán mas consientes al momento de digitar sus claves y compartir información sensible. Además de esto, se debe asegurar que la información de las claves de todos los usuarios se encuentre correctamente cifrada y aislada de modo que para un usuario común no sea un proceso sencillo encontrar este archivo y, aun cuando se logre acceder, se debe notificar cada ves que alguien accede o modifica este archivo para realizar un bloqueo inmediato en caso de ser necesario. Para que los usuarios puedan hablar con el servidor, debe ser necesario utilizar la llave antes mencionada por lo que es requerido que exista una comunicación encriptada entre cada actor.

4. Acceso no autorizado al sistema (Instalación de software malicioso):
   Para lograr prevenir que esto pueda ocurrir, primero se sugiere una identificación de usuarios como en el punto 1 pero además se sugiere adquirir un sistema de antivirus y/o Firewall robusto y en continua actualización que permita identificar rápidamente posibles amenazas y bloquearlas. En caso de que ya exista esta amenaza, se recomendaría un antivirus que este en continuo monitoreo verificando posibles patrones irregulares en la herramienta. Ya que los antivirus se alimentan también de datos históricos, es posible identificar con estos los virus que ya han sido inyectados en otras plataformas y que se han encontrado, por lo que es indispensable realizar una actualización periódica y un mantenimiento adecuado de esta herramienta.