**Caso 2 – Canales Seguros. Logística y Seguridad Aeroportuaria**

1. **Análisis y entendimiento del problema**

Suponiendo que el sistema descrito en la problemática cuenta con un firewall que filtra paquetes a la entrada de la red y antivirus en todas las máquinas de la compañía:

* 1. 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?

Los datos que deben ser protegidos son:

* + - **Información de los clientes para Novasoft financiero online:** Mantener un excelente nivel de confianza y evitar que sus datos sufran de espionaje por parte de personas sin autorización, para no permitir que se pierda la credibilidad en la buena reputación de Seguridad Aeroportuaria S.A.
    - **Información de los proveedores:** Asimismo, al almacenar información que hace referencia a otras empresas que proveen de servicios/productos a Seguridad Aeroportuaria S.A., se puede ver afectada la calidad del servicio de la empresa si las relaciones con sus proveedores se deterioran.
    - **Credenciales de usuarios:** Las credenciales de aquellos empleados o clientes que tengan acceso a la aplicación deben estar altamente aseguradas, pues en dado caso que alguien las obtuviera, se vería afectada significativamente la empresa, pues el acceso a toda la información que se maneja desde Novasoft en línea sería demasiado fácil, además de que se podrían afectar los otros servicios que trabajan en línea, dándoles de baja en la red o modificándolos.
    - **Tesorería:** Es importante proteger esta área ya que contiene toda la información relacionada con las operaciones de flujo de caja de la empresa. Entre estas, movimientos como cobros por actividades de la empresa, pagos realizados a terceros y gestiones bancarias. Si un actor no autorizado logra tener acceso a esta información podría afectar la eficiencia y eficacia los recursos financieros de la entidad. De este modo, se daría lugar al espionaje por parte de personas/organizaciones que quieran afectar la compañía.
    - **Cuentas por cobrar:** Esta información involucra tanto a la propia empresa como a los clientes y otros deudores. Por lo tanto, al no estar bajo un nivel adecuado de seguridad se podrían afectar las relaciones establecidas con los clientes. Entonces, si una persona no autorizada accediera a la información podría adulterar el estado de estas cuentas, y al mismo tiempo espiar la información sobre aquellos deudores de la empresa ocasionando que la confianza que estos tengan en la misma se vea afectada.

* + - **Cuentas por pagar:** Dado que las cuentas por pagar hacen referencia a los pasivos corrientes, al permitirse el acceso de terceros que busquen hacerle daño a la empresa, se podrían adulterar los datos correspondientes a dichas cuentas y esto conllevaría a una posible pérdida de dinero. También podría pasar que al conocer la información de las empresas a las que se les debe dinero se daría lugar a una suplantación por parte de alguien que quiera hacerse pasar por aquellas empresas asociadas a Logística y Seguridad Aeroportuaria S.A. y perjudicar las relaciones establecidas.
    - **Facturación:** Se debe proteger la información contenida en facturaciónya que representa los distintos movimientos de compras y ventas en la empresa. Así, en caso tal que la información sobre los activos fijos fuera vulnerada, estos datos servirían como un recurso para recuperar la información adulterada y de cierta manera equilibrar la inconsistencia que se pueda presentar.
    - **Compras:** Es importante llevar el control sobre los ingresos de la empresa, por lo cual, si estos datos son vulnerables, al ser manipulados por una persona inescrupulosa se pueden presentar problemas de repudio por parte de un cliente, en dado caso que se eliminen las compras que lo comprometen, justificándose en que este no realizó dicha compra porque no existe ninguna prueba, haciendo así, que Seguridad Aeroportuaria S.A. pierda dinero.
    - **Activos fijos:** Es importante llevar un control específico de los bienes tangibles e intangibles de la empresa, ya que, como empresa de seguridad aeroportuaria, existen ciertos recursos de los que sólo la misma empresa debe tener conocimiento. Si no está asegurada esta información, alguna persona o empresa con malas intenciones que logre acceder a ella podría afectar su funcionamiento operativo.

En resumen, todos los datos que hagan referencia a la parte de gestión financiera de la empresa son de vital importancia para su sostenibilidad con el paso del tiempo, debido a que esta información es periódicamente analizada y con base en esta se toman decisiones primordiales en la empresa.

Por otro lado, para los datos referentes a usuarios (clientes, empleados) y empresas vinculadas con la organización su seguridad es indispensable para la reputación de la empresa, para que la confianza del público se mantenga y nuevos clientes se vean atraídas por dicha seguridad.

Los principales problemas que se presentarían en la empresa al no asegurar la información anteriormente mencionada, serían principalmente espionaje, suplantación, adulteración y repudio.

* 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. Nota: Sus explicaciones DEBEN estar relacionadas con el contexto del problema planteado (las justificaciones indicarán cómo). NO se aceptarán respuestas genéricas.
* Transmisión de datos no cifrados de los clientes y/o proveedores, comprometiendo datos sensibles que pueden materializar riesgos de sabotaje a la operación o robo a la propiedad de los clientes o la empresa. Esto debido a la posibilidad de realizar ataques de eavesdropping y obtener la información sin cifrar.
* Almacenamiento sin cifrar en la plataforma de integración de los datos que se reciben de las sedes. Así como el almacenamiento no cifrado de los datos de los clientes y/o proveedores. En este caso la vulnerabilidad expone los datos en forma directamente interpretable para cualquier actor, malicioso o no, que tenga acceso a los registros del sistema (de manera física o remota).
* Errores de configuración del servidor central que permitan el acceso a configuraciones financieras inconsistentes. Dada la gran cantidad de sedes que maneja la empresa, la cantidad de información que debe manejar el servidor de la aplicación y la necesidad de centralizar esta información existe el riesgo de que, al realizar la integración de datos, sobre todo con las sedes internacionales a través de la versión offline, se presente inconsistencia de datos debido a la manera que se almacena información en cada una de las aplicaciones (Tienen su propia base de datos).
* Implementación de sistemas de cifrado inseguros (ya vulnerados) en los procesos de protección de datos sensibles o contraseñas, así como el uso de políticas laxas para la asignación de contraseñas de usuarios con acceso a información sensible. Esta vulnerabilidad permite que se asignen contraseñas especialmente sencillas de descifrar utilizando diferentes métodos como ataques de diccionario e ingeniería social, puesto que no hay políticas estrictas para el control de las posibles contraseñas (password strength); lo que junto al uso de sistemas inseguros de cifrado permiten que un atacante obtenga acceso al sistema y su información sin mayor dificultad. Este escenario es especialmente peligroso ya que hay una falsa sensación de seguridad sobre el sistema.

1. **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.

* Transmisión de datos no cifrados: La implementación de un mecanismo que represente de manera segura la transmisión de datos, esto podría hacerse mediante un cifrado asimétrico para obtener una llave de sesión simétrica que de paso a poder usar cifrado simétrico para enviar los mensajes de manera segura. Así, después de conocer y verificar la identidad del cliente, el servidor principal envía la llave de sesión en un sobre digital firmado con su llave privada, y el cliente después de verificar la identidad del servidor, utiliza esta llave para las comunicaciones por medio de un cifrado simétrico con la misma. De esta manera, gracias al procedimiento anterior, se garantiza la seguridad de los datos durante su transmisión.
* Almacenamiento sin cifrar: Encriptar datos importantes que estén guardados, usando algoritmos que no han sido vulnerados hasta el momento y logren proteger la información de manera eficiente. Para cumplir estándares de calidad internacional del nivel que lo requiere la empresa y que amerita los datos. Para poder escoger los datos importantes a cifrar, estos se deben clasificar por su nivel de relevancia, de esta manera se garantiza que sean los datos que más necesidad presentan de ser asegurados y a su vez, no se vea afectado el costo de la implementación ni el desempeño de la plataforma online de Seguridad Aeroportuaria S.A.
* Errores de configuración del servidor central: Se propone realizar barreras de acceso más duras para el servidor central, desactivando las cuentas por defecto del sistema, y de los diversos mecanismos, plataformas y frameworks usados durante todo el proceso, en caso de que esto sea imposible, usando contraseñas nuevas con alto nivel de seguridad. De igual manera, los permisos de cada usuario deben ser los mínimos necesarios para poder realizar las tareas designadas para sus usuarios. Así mismo, se deben especificar reglas de acceso y roles de usuario para que cada usuario solo use la información primordial de su interés, cambiando los permisos de lectura o escritura a la que se necesite para la terea. Con estas herramientas se garantiza que cada usuario tenga a su disposición solo su información y la de sus tareas.
* Datos sensibles o contraseñas: Manejar estándares (caracteres especiales, mayúsculas, números, etc.) para controlar el nivel mínimo de seguridad en las claves y/o credenciales para acceder al sistema, así como un tiempo de recomendación prudente para cambiarlas. Con esto se logra resistir a ataques de fuerza bruta para que un tercero pueda conseguir los datos válidos para acceder al sistema. Para que esto de resultados óptimos, los algoritmos escogidos para proteger la información deben ser certificados bajo altos estándares de calidad. Así, se asegura poder alcanzar un nivel de eficiencia y de seguridad ideal. Por último, se recomienda no tener en cuenta algoritmos actualmente vulnerados o implementados de manera independiente.