Juan Pablo Rocha – 201611835

Carlos Eduardo Robles - 201617129

Caso 2: Análisis y Entendimiento del Problema

1. Identificación y descripción de datos que deben ser protegidos:

   En un sistema de gestión empresarial y operativa de una compañía transportadora, en el área de rastreo de unidades de distribución, los datos utilizados deben ser protegidos son los siguientes:

   a. Datos de gestión administrativa: De estos datos depende la organización de información de proveedores y compras, activos físicos e infraestructura de la empresa. Si estos datos llegan a sufrir de errores de seguridad, aquel que logre ingresar a los datos podrá alterar la información crítica de la empresa, logrando eliminar datos importantes como gastos operacionales, trayendo consigo consecuencias negativas en la gestión financiera.

   b. Datos de gestión financiera: Estos son datos fundamentales en la empresa, de estos dependen el manejo contable y de recursos de los clientes y proveedores, así como la contabilidad general de la empresa, como lo sería comprobantes de cartera, cuentas por cobrar entre otros. Si una persona que no está autorizada logra acceder, estos datos estarían en grave riesgo de ser alterados, logrando consecuencias negativas importantes para la empresa si estos datos alterados fueran indicadores financieros tales como el balance general. Esto causaría que el modelo estratégico de negocio se vea alterado y por ende se correría el riesgo de que la empresa presente fraudes fiscales y tributarios.

   c. Datos de gestión comercial: Estos datos son los que determinan la actividad comercial de la empresa, manejando datos de clientes como facturación entre otros. Si se llegase a encontrar una vulnerabilidad de seguridad sobre estos datos, la empresa correría el riesgo de que la información de sus clientes sea alterada, así como de convenios y datos fiscales generales.

2. Identificación de vulnerabilidades:

   a. Uso de algoritmos propios de cifrado: Debido a que estos algoritmos son propios, no se puede tener confianza de ellos ya que no se han puesto a prueba en la vida real y no se conoce el nivel de seguridad al que estos podrían llegar.

   b. Daño en infraestructura tecnológica: La empresa transportadora tiene en su oficina principal tres servidores que manejan casi en su totalidad a toda la empresa. Eso trae consigo el riesgo de que algunos de estos servidores sufran de daños físicos por mala operación entre otras situaciones.

c. Integración continua: Debido a que cada 180 segundos las unidades se están comunicando con el servidor para informar su estado, esta integración continua de la información hace que sea vulnerable a ataques, dejando como consecuencia errores o registros falsos de información, impactando a los reportes financieros de la empresa.

d. Distribución de los algoritmos de cifrado: Debido a que cada aplicación tiene su propio archivo de configuración de usuario y cifrado que implementan algoritmos propios, estos algoritmos deberán ser distribuidos para todos aquellos que necesiten datos de las aplicaciones. Al no especificar que estas distribuciones son protegidas, se podrían interceptar por un tercero y posteriormente cifrar y descifrar la información de cada aplicación.

3. Mecanismo de resolución de vulnerabilidades:

a. Uso de algoritmos propios de cifrado: Se podría solucionar esta vulnerabilidad utilizando algoritmos de cifrado ya usados y probados, los cuales se han determinado que el nivel de seguridad es óptimo.

b. Daño en infraestructura tecnológica: Se propone el fortalecer los servidores con copias de seguridad o réplicas para que se esté con mayor tranquilidad al momento de un eventual daño en la infraestructura tecnológica. También se podría utilizar *cloud computing*, que garantice integridad, disponibilidad y seguridad de los datos.

c. Integración continua: Se recomienda que la información sea cifrada al momento de ser enviada, dando un poco más de tiempo entre cada uno de los envíos por parte de las unidades.

d. Distribución de los algoritmos de cifrado: Esto se solucionaría si previamente la empresa concuerda con qué algoritmo se va a cifrar y descifrar los datos y que estos sean estándar. Otra solución será que estos algoritmos sean cifrados con sus determinadas llaves.