**Caso 2**

ISIS 2203 Infraestructura Computacional

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

**1.** Identifique y describa los datos que deben ser protegidos en el sistema de rastreo de unidades de distribución. Explique su respuesta en cada caso y responda la pregunta ¿Si un actor no autorizado consigue acceso al dato mencionado, ya sea en modo lectura o escritura, cómo podría afectar la empresa?

Los datos que deben ser protegidos son:

* **Información contable**

Es importante proteger esta área ya que contiene toda la información relacionada con la contabilidad de la empresa. En esta área se encuentran movimientos como pagos realizados a terceros, gestiones bancarias y cobros por actividades de la empresa, entre otras. Si un actor no autorizado logra tener acceso a esta información, podría afectar la actividad financiera de la compañía y, por ende, la razón social de la misma. Así las cosas, aquellas personas u organizaciones que deseen afectar la compañía podrían realizar espionaje.

* **Información asociada al rastreo de la distribución de paquetes**

Es importante tener especial cuidado con la información relacionada al rastreo de distribución de paquetes de la compañía pues el rastreo permite realizar un seguimiento continuo de las operaciones de la empresa, de manera que se verifique el cumplimiento de los procesos de negocio de la compañía. Si una persona no autorizada accede a la información de rastreo de la distribución de paquetes podría modificarla y así afectar la entrega, lo cual generaría problemas con los clientes y esto afectaría en la credibilidad y situación financiera de la empresa.

* **Credenciales**

Se necesita proteger las credenciales de aquellos empleados o clientes que tengan acceso a la aplicación, pues en dado caso que alguien las obtuviera se vería afectada significativamente la empresa, debido que el acceso a toda la información que se maneja en el sistema sería demasiado fácil, además de que se podrían afectar los otros servicios que trabajan en línea, dándoles de baja en la red o modificandolos.

* **Información de los usuarios**

Es necesario proteger la información de los usuarios puesto que es vital 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 la compañía transportadora.

En conclusión, todos los datos que hagan referencia a la situación financiera de la empresa son de importancia en el proceso de toma de 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, de manera que la confianza del público se mantenga y fortalezca, 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.

**2.** Identifique cuatro vulnerabilidades de ese sistema, teniendo en cuenta únicamente aspectos técnicos o de procesos (no organizacionales). Identifique vulnerabilidades no solo en lo relacionado con la comunicación sino también con el almacenamiento y procesamiento de los datos. Explique su respuesta en cada caso.

* Transmisión de datos no cifrados de los clientes, pues existe la posibilidad de realizar ataques de espionaje y obtener la información sin cifrar, comprometiendo datos sensibles que pueden materializar riesgos de sabotaje a la operación Así mismo, puede haber robo de identidades que afectan la situación de la empresa al otorgar privilegios asociados a la identidad nueva. Por otro lado, esta vulnerabilidad afectaría también al usuario que sufre suplantación puesto que el atacante puede acceder a información bancaria del usuario, por ejemplo, realizando movimientos de dinero importantes.
* Acceso no autorizado al sistema, con esto se podría dar que una persona no autorizada logre entrar a información sensible de la empresa, pero también podría realizar la instalación de un virus o malware en el sistema con el cual pueda mantener un acceso directo a los datos de la empresa y de los usuarios. Esta vulnerabilidad puede ser bastante grave debido la cantidad de datos a la cual es posible acceder.
* Acceso a la información contable que permitan la lectura y/o la modificación de la información de la situación financiera de la empresa, que conlleva a configuraciones financieras inconsistentes. Dada la gran cantidad de sedes que maneja la empresa, la cantidad de información que debe manejar el servidor de manejo administrativo y la necesidad de centralizar esta información, generan riesgo a la hora de realizar la integración de datos, pues puede presentarse inconsistencia de datos que afectan la situación financiera de la empresa.
* 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.

**3.** Para cada una de las vulnerabilidades que usted identificó en el punto anterior, proponga mecanismos de resolución.

a. Los mecanismos propuestos deben ser explicados. Por ejemplo, si se habla de cifrado sobre un canal de comunicaciones, debe identificar los participantes en la comunicación, y si es cifrado simétrico o asimétrico (y justificar la decisión).

b. Además, debe explicar por qué resuelve la vulnerabilidad identificada

* Transmisión de datos no cifrados: La solución de esta vulnerabilidad radica en la implementación de un mecanismo que represente de manera segura la transmisión de datos. Lo anterior podría realizarse mediante un cifrado asimétrico para obtener una llave de sesión simétrica que permita hacer cifrado simétrico para enviar los mensajes de manera segura. De esta manera es posible verificar la identidad del cliente para que, posteriormente, el servidor principal envíe la llave de sesión en un sobre digital firmado con su llave privada. Así, el cliente puede verificar la identidad del servidor y usar esta llave para comunicarse mediante cifrado simétrico con ella. Es así como la vulnerabilidad planteada en el punto anterior puede ser resuelta.
* Acceso no autorizado al sistema: Para prevenir esta vulnerabilidad se sugiere una identificación de los usuarios para así poder controlar la autenticación y la autorización de cada uno, pero además adquirir un Firewall robusto, el cual tenga una constante actualización para así identificar rápidamente amenazas y bloquearlas. Si esta amenaza ya existe, se recomienda tener un antivirus que haga un monitoreo continuo en busca de patrones irregulares en el sistema. Como ya se dijo anteriormente, es necesario realizar una actualización y mantenimiento periódico y adecuado ya que estas herramientas se alimentan de datos históricos y casos parecidos en otras plataforma. Como ya se mencionó anteriormente, es necesario que estas herramientas tengan una actualización periódica, debido que gracias a la alimentación de datos históricos que usan los antivirus se podrían identificar virus encontrados en otras plataformas.
* Acceso a la información contable: La solución recomendada para solucionar esta vulnerabilidad es implementar un sistema de seguridad por medio de cifrado o la actuación de un tercero que asegure la integridad de los datos. En caso de implementar la primera solución, el atacante no puede interpretar la información si no cuenta con la llave de desencriptación para su lectura. Por el contrario, la segunda opción facilita el manejo de seguridad, puesto que le asigna a un tercero la responsabilidad de prestar atención a cualquier posible vulnerabilidad del sistema. Así mismo, le otorga a la compañía transportadora la posibilidad de invertir más tiempo en otros procesos importantes para la empresa. Por medio de estas dos alternativas, se reducen los problemas de autenticación y se garantiza la seguridad de la información para los clientes de la compañía.
* Datos sensibles o contraseñas: La solución implica adquirir políticas más estrictas como el manejo de estándares, como caracteres especiales o mayúsculas, para aumentar el nivel de seguridad en las credenciales para acceder al sistema, así como un tiempo de recomendación prudente para cambiarlas. Con esto se logra resistir a ataques de fuerza bruta por parte de un tercero, para conseguir los datos válidos para acceder al sistema. Para que esta solución sea efectiva, 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. Se aconseja cambiar aquellos algoritmos que fueron vulnerados, para disminuir un poco el riesgo.