**Caso de Estudio 2 – Canales Seguros**

**Logística y Seguridad Aeroportuaria**

Entregado por:

Sergio Madera, código 201417957

Andrés Zuleta, código 201413405

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

En el sistema descrito en el párrafo anterior:

1. Identifique y describa cinco amenazas al sistema descrito en los párrafos anteriores. Explique su respuesta en cada caso (\*) y responda la pregunta ¿Si la amenaza se consolida, cómo afectaría al sistema?

* Disponibilidad: En el sistema no se describieron balanceadores de carga o estructuras similares, por lo que cada uno de los servidores por separado sería vulnerable a la sobrecarga por un uso excesivo de los usuarios legítimos o a ataques de negación de servicio (DoS) perpetrados por entes externos con la intención de interrumpir o ralentizar temporalmente las actividades de la compañía. No obstante, dado que el servidor que maneja el sistema financiero, el cual es el más crítico de los descritos para la operación de la empresa, es capaz de trabajar offline, el riesgo de un ataque remoto de este tipo se ve reducido enormemente. A pesar de esto, si la seguridad de uno o varios de los ordenadores de la compañía con la capacidad de acceder a este sistema no es suficiente se puede instalar un software que, al detectar que se envía una transacción al servidor, amplifique este comando en el intento de sobrecargarlo. De realizarse la amenaza de interrupción de servicio, en el peor de los casos se vería caído el servidor encargado del sistema financiero, y no se podría acceder, actualizar o modificar ningún dato concerniente al estado financiero de la empresa. En otras palabras, no se podría realizar ninguna acción sobre los registros de compras, facturación, pagos, entre otras piezas de información vitales para el funcionamiento diario de “Logística y Seguridad Aeroportuaria S.A.”
* Integridad: Fue descrito que se verifica la autenticación de usuarios en los servidores uno y dos, pero no se especificó nada sobre la verificación de la integridad de los paquetes de información enviados y recibidos durante una transacción. Esto quiere decir que si al realizar una transacción para un usuario los paquetes de datos pasan por otro servidor intermedio que no sea lo suficientemente seguro, es posible modificar la información que llega al usuario o la transacción que llega al servidor. Lo anterior mencionado significa que sería posible modificar datos financieros y/o aquellos concernientes al sistema Time & Attendance o la información de interés general que muestra el servidor tres sin la necesidad de obtener los privilegios para realizarlo dentro del sistema, esto es, obtener las credenciales de un usuario autorizado. No obstante, aún se deben obtener de alguna forma los derechos para interferir con el flujo de datos entre el emisor y el receptor en el sistema intermediario, lo cual podría ser reaizado con algún tipo de software espía instalado en un nodo con poca seguridad de dicho sistema intermedio. De completarse la amenaza, sería posible para el atacante enviar información no solicitada o errónea al usuario, e incluso atrapar la información correcta para sí mismo. Sin embargo, incluso si el atacante no posee los medios para descifrar o modificar de forma sensible el flujo de información que intercepta, puede agregar bytes aleatorios a dicho flujo, ocasionando que el sistema receptor no sea capaz de leerlo correctamente; ello tendría un efecto disruptivo sobre el funcionamiento consistente de la aplicación, afectando y disminuyendo la productividad laboral de la compañía. En adición a esto, se comenzaría dudar de la veracidad de los datos provistos por la plataforma y de la capacidad de la empresa para mantener los mismos seguros, efecto que persistiría incluso después de cubierta la brecha en la seguridad.
* Confidencialidad: Si la información referente a los datos de autenticación en los servidores uno y dos de los usuarios no es resguardada de una forma lo suficientemente segura, un agente externo podría hacerse con las credenciales necesarias para hacerse pasar por alguien autorizado para realizar cierto tipo de transacciones. En consecuencia, agentes no autorizados podrían obtener privilegios sobre información confidencial en el sistema financiero o el sistema Time & Attendance. Una posibilidad para el robo de las credenciales de un usuario autorizado sería si, por ejemplo, uno de estos intenta acceder al sistema a través de un equipo con un troyano instalado anteriormente; este equipo podría ser incluso el computador personal del usuario, el cual fue infectado sin que este se percatara de ello. De consolidarse la amenaza, una parte potencialmente importante de la información privada de la empresa sería obtenida o modificada por agentes externos con intenciones posiblemente maliciosas, lo que podría amenazar la existencia estable de la organización como tal. Esto es especialmente cierto si el servidor cuya seguridad fue violada fuera aquel responsable del sistema financiero, pues se podría obtener información crucial sobre la contabilidad, facturación, compras, activos fijos, entre otros.
* Autentificación: En el párrafo fue descrito que los servidores uno y dos solicitan la autenticación de un usuario autorizado, y sólo realizan transacciones para ellos. Sin embargo, no se hicieron afirmaciones sobre el registro de las acciones que realiza cada uno de los usuarios, en especial de las transacciones que genera. Este tema está fuertemente ligado a la confidencialidad, de la que se habló anteriormente, pero se refiere a la forma de rastrear posibles brechas ya existentes en la seguridad al tener la capacidad de probar el autor de cierto paquete de información, con lo que se podría desenmascarar a un agente interno con intenciones maliciosas, que espera actuar sin que sus pasos puedan ser rastreados hasta él. De consolidarse la amenaza, un agente malicioso podría modificar o borrar información ya existente, lo cual es especialmente peligroso si es información referente al sistema financiero que maneja uno de los servidores, y sería imposible encontrar al culpable de estas acciones, dejándolo libre para actuar de nuevo en contra de “Logística y Seguridad Aeroportuaria S.A.”
* No-repudio: En la estructura descrita, no se realizaron afirmaciones sobre la capacidad del sistema para probar que una pieza de información fue en efecto enviada por un cierto emisor y/o recibida por un cierto receptor. De consolidarse la amenaza en en el contexto planteado, una posibilidad para explotar la brecha de seguridad para un agente con intenciones maliciosas dentro de la empresa sería la capacidad ignorar activamente alertas importantes del sistema, dejando que su estado potencialmente empeorara con el tiempo y luego afirmar que nunca recibió tales alertas. Por otro lado, también se podría consolidar la amenaza si un agente con intenciones maliciosas obtiene de alguna forma una transacción o un paquete de datos no verídico y/o posiblemente nocivo para el sistema generado por un autor diferente de sí mismo, y luego envía dicha información; de esta forma, ya que no es posible probar el verdadero emisor, toda la culpa caería sobre quien generó los datos, dejando al real culpable libre para seguir afectando la compañía y sus operaciones. De esta forma, se podrían inculpar a empleados importantes para la empresa de inyectar información fraudulenta a los servidores que manejan el sistema financiero o el sistema Time & Attendance, razón por la cual la organización se vería obligada a despedirlos y a reparar el daño realizado cada vez. Ello representaría un desgaste gradual para “Logística y Seguridad Aeroportuaria S.A.”, empeorando su capacidad de reacción al cambiante mercado.

1. Identifique cinco 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 y procesamiento de los datos. Explique su respuesta en cada caso (\*).

(\*) *Sus explicaciones DEBEN estar ligadas al contexto del problema planteado e indicar cómo. NO se aceptarán respuestas para contextos genéricos.*

* En el párrafo no se realizaron aclaraciones sobre los derechos que un usuario tendría sobre los ordenadores de la empresa que los empleados utilizan frecuentemente para acceder al sistema. En consecuencia, sería posible para los mismos instalar y configurar programas de su elección en dichos ordenadores, por lo que podrían ingresar software espía al sistema con la intención de robar las credenciales de los usuarios. En el caso de los usuarios autorizados para realizar transacciones en los servidores encargados del sistema financiero y el sistema Time & Attendance, esto presenta una amenaza aún mayor.
* En el sistema no se describió si por la forma en la que estaba implementado se impedía la descarga de información desde el servidor, de quién tendría derechos para hacerlo o de cómo se guardaría esta información descargada. Por lo tanto, si un usuario autorizado descarga información del servidor y esta no está cifrada al guardarse, un agente con intenciones maliciosas podría descargar la información a escondidas y acceder a ella sin necesidad de tener también que, por ejemplo, pasar por la prueba de seguridad de obtener la llave de este usuario, el cual podría ser el caso si la información se guardara encriptada.
* No se describe el comportamiento de los servidores frente al ingreso de una gran cantidad de datos a la base de datos en un corto periodo de tiempo. Por esta razón, si esto llegase a suceder, existe la posibilidad de que el servidor intentara alocar más información de la que es capaz de alocar físicamente, ocasionando que la información anterior se volviera corrupta e ilegible. También es posible que el servidor simplemente se negara a borrar la información anterior o enviarla a otra localización para archivarla y dejase de recibir transacciones que ingresaran más datos al sistema, lo que ralentizaría la operación de la empresa.
* En la página no se describen los medios por los cuales los mismos servidores o entidades diferentes son capaces de detectar si hay algún problema de disponibilidad con el sistema. Por esta razón, si alguno de ellos se llegara a caer, sería necesario que un humano se diera cuenta del problema y luego que el departamento de TI de la compañía comenzase a trabajar para que el sistema vuelva a estar en línea. Este proceso puede tardar horas, lo que le costaría una cantidad considerable de dinero a la compañía.
* Una vulnerabilidad posible del sistema descrito son las contraseñas de los usuarios. En el párrafo no se define ninguna regla respecto a las contraseñas que pueden tener los usuarios autorizados, por lo que, en algunos casos, estos pueden tener contraseñas muy cortas o muy sencillas, lo que haría que realizar un ataque de fuerza bruta para conseguir sus credenciales no sería realmente complicado por parte de un agente con intenciones maliciosas.

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

Para cada una de las amenazas que usted identificó en el punto anterior, proponga mecanismos de resolución/mitigación.

* 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).
* Además, debe justificar los mecanismos propuestos. Es decir, identifique explícitamente cuál riesgo mitiga y cómo.

En sus justificaciones tenga en cuenta aspectos relacionados con eficacia, costo, eficiencia, flexibilidad, aspectos de implementación, y otros aspectos técnicos que considere convenientes.

* Disponibilidad: Para mitigar el riesgo de ataques de negación de servicio y al mismo tiempo aumentar la robustez del servidor frente a la carga inesperada del sistema, es necesario modificar la arquitectura actual de la aplicación de tal forma que hayan varios servidores capaz de manejar las transacciones enviadas al sistema financiero de forma concurrente, para hacer posible el balanceo de carga entre los mismos. Para implementar esta solución sería necesario comprar tantos servidores como nodos para balancear la carga se quiera poseer, además de uno, quizá de menor capacidad, que se encargase de balancear la carga entre los mismos. En adición, se deberá definir la forma en la que la carga será balanceada adaptar el software existente para realice dicho balanceo automáticamente entre los nodos disponibles y verificar que la forma en la que cada diferente nodo trata las transacciones de forma que cumplan todos los requerimientos de seguridad que un único servidor a cargo del sistema financiero, del sistema Time & Attendance o de presentar información de interés general lo haría.
* Integridad: Para mitigar el riesgo de integridad de la información se puede encriptar cada paquete de datos en el momento inmediatamente anterior a su envío utilizando un código de hash criptográfico. El receptor ha de aplicar la misma función de hash criptográfico al objeto recibido y verificar que el código de hash generado por el objeto al momento de recepción sea igual a aquél generado por el objeto al momento del envío. De lo contrario, se deduciría que se realizó algún cambio en el objeto durante su envío, y se considera que el paquete recibido no es confiable. Para implementar esto sería necesario modificar la forma en la que cada servidor existente maneja las transacciones que recibe por parte de los usuarios. Esto se dificulta en los servidores que manejan el sistema financiero y el sistema de Time & Attendance, puesto que para actualizar el programa existente se ha de alargar el tiempo de mantenimiento de los mismos. No está de más aclarar, sin embargo, que esta medida aún será vulnerable al método de adición de bits aleatorios a cada flujo de información, con el cual sería posible hacer que muchos paquetes de datos recibidos fueran “poco confiables”, y ocasionando que fuera necesarios pedirlos de nuevo al servidor. A pesar de ello, mitiga los efectos que puede tener sobre los datos guardados en el sistema, al tiempo que es una alternativa de bajo costo y no afecta en gran medida el tiempo de respuesta.
* Confidencialidad: Respecto al riesgo de confidencialidad, se propone como medida de mitigación la educación continuada de cada uno de los usuarios autorizados para interactuar con archivos con requerimiento de confidencialidad para que sepan reconocer lugares seguros para utilizar sus credenciales y conectarse al sistema. En adición, se propone la prohibición de instalar cualquier tipo de aplicación en los ordenadores de la empresa sin una autorización del más alto nivel de seguridad para evitar la inserción de spyware o programas de naturaleza similar dentro del sistema. La educación continuada de los usuarios autorizados requerirá esfuerzos de diseño para poder presentar información al respecto de forma no invasiva, con el objetivo de no tener un efecto disruptivo sobre sus actividades normales; ello se podría traducir en un gasto económico por un diseño que redujera la productividad de los empleados o un gasto económico para contratar a un tercero capaz de garantizar un buen diseño para la adición. Respecto a la prohibición de instalación de programas sobre los ordenadores de la empresa, es una solución de bajo costo que el departamento de TI podría realizar rápidamente; no obstante, los empleados perderían parte de su autonomía, pes tendrían que utilizar únicamente los programas provistos por la empresa para llevar a cabo sus funciones.
* Autentificación: Para mitigar el problema de autentificación se propone la generación de una llave privada y una llave pública para cada uno de los usuarios autorizados para realizar transacciones en los servidores uno y dos, además de la educación de dichos usuarios para proteger su llave privada y guardarla en un lugar seguro. Utilizando este par de llaves se hace posible la implementación de una firma digital única para cada usuario, con lo que sería posible probar la autoría o proveniencia de cualquier paquete de datos y/o transacción realizada por el servidor. Esta solución requiere, no obstante, que los empleados entiendan la importancia de proteger su llave privada para ser efectiva, concepto que puede ser difícil de entender. Además, la modificación a la forma en la que tanto el ordenador emisor como el servidor receptor y viceversa tratan la transacción no es trivial, por lo que presentaría una carga considerable para el departamento de TI de la empresa y tardaría cierto tiempo en diseñarse y desarrollarse.
* No-repudio: Concerniente a la mitigación del riesgo de no repudio se propone la participación de un tercero de confianza que modifique el sistema de tal forma que sea capaz de acceder al mismo y de alguna forma verificar que las firmas de cada uno de los archivos sea verídica o no; para que esta solución sea más eficiente, se ha de implementar en conjunto con la propuesta para mitigar el riesgo de autentificación. Así, sería posible para el tercero confiable confirmar que el emisor es efectivamente el autor del paquete de datos enviado, al tiempo que confirma quién es el receptor. Esto sería difícil de lograr puesto que un tercero realmente confiable no sería sencillo de encontrar, además del costo económico que representa el tiempo que el servidor se encontrará el mantenimiento y el servicio continuado que ha de prestar dicha entidad de confianza. En adición, la propuesta es poco flexible y aumentaría los posibles puntos de entrada para que se efectúe una brecha de seguridad, dado que se podría acceder al sistema de “Logística y Seguridad Aeroportuaria S.A.” a través del tercero.