Juan Sebastián Prieto - 201426358

David Joel Bautista - 201512756

Julián Andrés Bermúdez - 201519648

Caso II

Parte A:

Amenazas:

* no disponibilidad: la aplicación historial laboral, es una aplicación disponible en línea, la cual cuenta con una gran cantidad de transacción diarias y su nivel de procesamiento es muy alto, esta aplicación debe contener un nivel de disponibilidad muy alto por todas las características nombradas anteriormente por lo que una amenaza de esta aplicación es que puede quedar en un estado fuera de línea si se sobrecargan los servidores.
* corrupción: debido el tipo de información que maneja la aplicación en general cuenta con un alto riesgo de corrupción por parte de personas ligadas a la empresa, ya sea empleados que manejan la información de las transacción o directivos de alto nivel los cuales tiene privilegios sobre cierto tipo de información de esta manera podría modificar esta información para beneficio personal. Esto puede ocurrir debido a que Colpensiones es una empresa grande por lo que una gran cantidad de personas podrían tener acceso a esta información
* adulteración: la aplicación historial laboral puede llegar a realizar hasta 5.500 transacciones por día. Teniendo en cuenta que la comunicación del cliente con los empleados es vía internet -la cual no es la forma más segura-, dicha conexión puede ser usado por alguien que tenga intención de vulnerar el sistema. Por lo que, debido a ese alto nivel de transacciones, tiene mayores posibilidades para adulterar las transacciones originales modificando sus valores.
* acceso a terminales: los terminales que usan los empleados podrían no estar protegidos de la mejor manera en lo que se refiere a su acceso físico. por lo que se podría acceder a la información de toda la oficina central de esta manera.
* lectura de información de base de datos (espionaje): la empresa cuenta con una gran cantidad de bases de datos y gigantescos volúmenes de información. al tener tanta información, de tanto empresas como personas, la base de datos debería garantizar que está información no pueda ser leída por ninguna persona aparte de la autorizada así que la información de las bases de datos debería estar encriptada.

Vulnerabilidades:

* no disponibilidad: La aplicación de historial laboral puede ser afectada en cuanto a su disponibilidad debido a que los servidores en general cuentan con un tiempo de uso, en la mayoría de los casos, mayor a 4 años y en algunos casos hasta 10 años. El servidor activo de la aplicación cuenta con una carga, en hora pico, de hasta 72% con algunos núcleos de CPU de hasta 92%. Además, con el agravante de que se estima que el servidor pasivo no pueda soportar la carga del servidor activo en caso de algún fallo, si llegara a ocurrir un sobrecargo en el servidor, la aplicación no se podría mantener en línea.
* penetrar la red: si bien oficina central de la entidad cuenta con una subred privada, existen 64 puntos de conexión con el centro de datos central, por lo que sí se lograra acceder a algún punto de esa red privada, de cualquiera de todos los puntos de conexión, se lograría obtener acceso a toda la información.
* adulteración: la comunicación entre los usuarios tipo empleado de las sucursales ocurren vía internet sin ningún tipo de cifrado para los mensajes, esto sucede de manera contraria al modo de comunicación con terceros la cual está fuertemente cifrada. El factor anterior puede ser problemático para la empresa porque cualquier mensaje se puede adulterar o espiar.
* acceso a terminales: si bien es cierto que los terminales cuentan con una autenticación para que los empleados puedan acceder a ella se podrían realizar ataques de fuerza bruta hasta poder acceder a los terminales.
* cifrado de bases de datos: La información de las bases de datos no está cifrada por lo que ante un robo de información no se puede garantizar que no se pueda realizar lecturas sobre la información.

Parte B:

Propuestas de soluciones:

* para poder mitigar esta amenaza de disponibilidad se debe empezar un proceso de cambio de servidores viejos por nuevos y re-potenciar los nuevos a su máxima capacidad, tal como lo recomendó el proveedor del manejador de la base de datos, con una configuración mínima de 256 GB de memoria RAM, esto lograría que la capacidad de procesamiento aumentará en gran medida provocando que la sobrecarga sobre los servidores disminuyera haciendo mucho menos probable un fallo por sobrecargo para que el servicio pueda seguir en línea normalmente
* para poder mitigar el problema de corrupción se cree que la mejor manera de por implementar mecanismos de protección, de tal manera que se limite los permisos de programas, procesos y usuarios a diferentes tipos de recursos, el mecanismo que se cree el cual es el más indicado para esta labor es la lista de capacidades por que verifica los permisos sobre los procesos esto evitaría que se pudieran hacer modificaciones sin los suficientes permisos, ocasionando que solo cierto tipo de usuario tenga permisos especiales sobre un tipo de información dada, al no ser un mecanismo de protección en anillos no es necesario que entre más alto sea el nivel de un empleado dentro de la empresa debe tener más permisos sobre las aplicaciones porque en realidad los directivos no necesitan acceso a todo, una lista de capacidades puede dar esta posibilidad de variar permisos.
* para poder solucionar la amenaza de la adulteración, se debe empezar a implementar comunicación cifrada de tal manera de que solo las partes que estén involucradas en la comunicación puedan obtener los mensajes y comprobar su autenticidad, la manera que se cree que se debe implementar esta solución es empezando a cifrar los mensajes con llaves asimétricas, primero con la llave pública del destinatario para que solo este pueda descifrar el mensaje con su llave privada, además al mensaje se le debe concatenar el resumen del mensaje cifrado con la llave privada de la fuente, con el propósito de verificar en primer lugar la autenticidad del documento y en segundo lugar la identidad de la fuente debido a que solo se podría descifrar el resumen con la llave pública de la fuente. Además, el cifrado por llave asimétrica no requiere el uso de tantos recursos
* para mitigar el acceso a los terminales: se debería implementar mecanismos de autenticación que impliquen biométricos así solo la persona autorizada podrá acceder a su terminal.
* para poder solucionar la amenaza de la lectura de información almacenada en las bases de datos, se cree que se debería implementar un mecanismo de cifrado de información, además se cree que el mecanismo más apropiado para este caso es un mecanismo de cifrado simétrico puesto que el cifrado no va encaminado a evitar espionaje en plena comunicación para que no requiere tanto nivel computacional, sino que se quiere a que si alguna persona pueda a llegar a tener acceso a las bases de datos no pueda hacer lecturas sobre ningún tipo de información.