Luis Miguel González Fernández
Mateo Saravia Salamanca
Santiago Gutiérrez Cano
Caso 2 Infracomp

A. Análisis y entendimiento del problema:

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?**

- **Contabilidad:** Este es un dato privado y personal para cada empresa porque la simple divulgación de estos datos ya afecta a la empresa; si alguien no autorizado llegara a conocer esta información podría provocar desfalcos, desviación de recursos, manipulación de datos para actos fraudulentos y/o provocar la caída de la empresa.
- **Presupuesto:** Al igual que la contabilidad este dato es privado y si se llegara a conocer afectaría la empresa además que es de mucha más importancia dado que si este valor se llega a saber por personas inescrupulosas podían intentar robar, sobornar o elevar costos por prestaciones de servicios.
- **Cuentas por pagar:** Para este caso las cuentas podrían generar problema porque no solo se está revelando información de la empresa sino también una manipulación para provocar inconsistencias afectando la contabilidad de la empresa.
- **Cuentas por cobrar:** El manejo de esta información debe ser cuidadoso, estas cuentas son aún más importantes que las cuentas por pagar. Estos datos no solo incluyen información de la empresa, también incluye información de clientes por lo que su mera divulgación afecta legalmente a la empresa; del mismo modo, la manipulación de estos datos afecta directamente la contabilidad de la empresa, provocando desfalcos y fraudes.
- **Datos de los usuarios:** Estos son los datos más importantes, puesto que implican la información más sensible y completa sobre los clientes de la empresa. La divulgación de estos datos afecta directamente a los clientes, ya que son prestos a un robo de credenciales y datos incluso bancarios;

además, implica problemas legales para la empresa adicional a una pérdida de confianza y mercado.

- **Facturación y Compras:** La filtración y manipulación de estos datos implica vulnerabilidades en medios de pago y credenciales, además de que estos datos son evidencia importante de los movimientos financieros y activos de la empresa, por lo que son vitales para evitar inconsistencias en contabilidad y cobros.
- **Activos Fijos:** Con esta información se puede conocer el pasado, vigilar el presente y programar el futuro de las inversiones del negocio, tanto a corto como a largo plazo, conocer información sobre inmuebles, inversiones etc. Además de que si estos son modificados podría llevar a la empresa a la bancarrota o ocasionar graves problemas de liquides.

2. **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.**
   - **Algoritmos poco seguros:** Usar algoritmos poco seguros puede resultar en una vulnerabilidad, ya que los datos encriptados no cumplen con los suficientes estándares y pueden ser fácilmente desencriptados y vulnerados. A su vez, estos algoritmos pueden ser poco eficientes, por lo que se pueden forzar caídas y ataques por este aspecto.
   - **Canales de comunicación:** Por este medio viaja información que se maneja en la empresa, por lo que interceptar uno de estos canales puede resultar en la filtración si además no están encriptados; adicionalmente, se puede enviar información malintencionada y modificar los datos al destino.

- **Control de acceso:** Si no se establece un buen control de acceso con jerarquías, datos importantes pueden ser accedidos por personal de bajo nivel, provocando manipulación indebida y exposición de datos sensibles a personal no autorizado.
- **Disponibilidad:** Dado el poco espacio actual de almacenamiento, basado en los usuarios esperados, no hay margen de error, por lo que los ataques (DDOS o DOS) serán un potencial peligro puesto que la prioridad de estos servicios es alta. Además, no se cuenta con un servidor de emergencia para mantener ese escenario de calidad en caso de caída.

B. Propuestas de soluciones

- **Algoritmos poco seguros:** Dado que para que los datos e información este seguro se tendría que utilizar algoritmos de encriptación para que estos viajen y en dado caso que sean interceptados no puedan descubrir su contenido. Se recomienda probar la seguridad de estos algoritmos bajo casos extremos y/o usar algoritmos conocidos que cumplan con estándares de seguridad, y que sean eficientes para que el rendimiento cumpla con la demanda de los usuarios; adicionalmente, se recomienda usar diferentes cifrados para diferentes conjuntos de datos para evitar la filtración completa de todos los datos una vez vulnerado el sistema.
- **Canales de comunicación:** La información más sensible debe viajar encriptada para disminuir al máximo la posibilidad de robo e interceptación de estos datos; sin embargo, los canales de comunicación deben ser de igual manera seguros, especialmente para el caso de NovaSoft online, ya que aquí es donde más posibilidades de ataques e interceptaciones hay. Estos canales deben ser asegurados mediante credenciales principalmente, además de usar protocolos certificados y conocidos para evitar interceptaciones por este medio. Otra manera es encriptar los datos menos importantes con algoritmos que se centren en eficiencia más que en seguridad.

- **Control de acceso:** Se debe estructurar de manera adecuada la organización de la empresa, y delegar niveles de acceso a la información. Cada actor de la empresa debe tener un usuario en el cual se especifica el nivel de acceso que posee, y basado en estas credenciales otorgar acceso a los diferentes canales e información de la base de datos. También se debe implementar control para evitar la suplantación de identidad, ya sea desde el interior como el exterior de la empresa y así incrementar la seguridad.
- **Disponibilidad:** Como primera medida para asegurar los diferentes escenarios de calidad, se debe tener un servidor de emergencia, con una reserva de los datos para mantener la disponibilidad al máximo; de igual manera, se debe dejar un margen de error en el espacio actual de almacenamiento para evitar una caída del servidor en especial en momentos críticos como ataques o alta cantidad de usuarios concurrentes. Otro aspecto importante es asegurar la información que todavía no ha sido persistida en base de datos, por lo que una caída en un momento de alta concurrencia provocaría perdida de datos masiva, de ahí la importancia de mantener la disponibilidad y resguardar la información en al menos dos bases de datos.