**Universidad de los Andes Ingeniería de Sistemas y Computación**

**Infraestructura Computacional**

**Trabajo Caso 2**

Presentado Por:

**Sebastián Salas 201225327**

**Nicolás Rozo 201225282**

**A Análisis y entendimiento del problema**

**Punto 1.**

**Información que debe ser protegida:**

1. **Información contable** que son los datos administrativos de la compañía. Se maneja la información en una intranet.
2. **Información del rastreo** de unidades distribuidas y su estado de entrega. Los datos se almacenan en los servidores.
3. **Información del manejo de órdenes** que contiene los datos de rastreo y rutas, de acuerdo a estos datos se podría recalcular las rutas. Esta información se realiza de acuerdo a la información la distribución de unidades.
4. Por último, **información de la comunicación entre los puntos de atención al cliente y servidores** que contiene los datos del estado del cliente.

**¿Si un actor no autorizado consigue acceso al dato mencionado, ya sea en modo lectura o escritura, cómo podría afectar la empresa?**

Suponiendo que se implementa control de acceso a nivel de sistema operativo en todos los servidores, y cuenta con un firewall que filtra paquetes a la entrada de la red, se afecta a la empresa de la siguiente manera:

1. En **el manejo de los datos contables**, si hay un acceso no autorizado puede afectar a la compañía en que se puede producir datos inconsistentes o espionaje. En el peor de los casos los actores toman datos personales de la empresa como los datos de cuenta o número de tarjetas de crédito y contraseñas.
2. En la **información de rastreo** de unidades de distribución puede producirse inconsistencia de información si alguien no autorizado modifica los datos. Esto puede afectar la empresa en los futuros cálculos de rutas donde se producen “condiciones excepciones” de cambio de rutas. ///
3. Un acceso a los **datos de manejo de ordenes** (rastreo y rutas), puede ocurrir espionaje de los datos funcionales de la empresa que sería el cálculo de rutas con base en los puntos de atención que han recibido paquetes. El robo de información que podría bien ser la propuesta de valor de la compañía podría ser usado por otras empresas para competir.
4. Un acceso a **los datos que se envían entre puntos de atención al cliente y servidor** puede ocasionar problemas de suplantación entre quienes se comuniquen o espionaje. Afecta a la empresa dado que se puede presentar inconsistencia en los datos de los servidores o los actores externos pueden conocer información de lo que se comunican entre los clientes y servidores.

**Punto 2.**

1. Los **datos administrativos** de la empresa pueden ser vulnerados en dado que un actor externo que no tiene permisos de acceso podría modificar los datos o la información puede ser disponible para personas no autorizadas. Esto debido a que dado que no hay datos cifrados en los servidores, agentes externos pueden conocer las contraseñas de los usuarios y autenticarse con un usuario valido al acceso de información con la contraseña extraída.
2. Los **datos de información de rastreo**  puede ser vulnerado de forma que diferentes unidades de distribución pueden hacerse pasar por unidades que no son, y al enviar datos al servidor genere datos inconsistentes.
3. Los **datos de manejo de ordenes**  pueden ser vulnerados en confidencialidad dado que solo la empresa debería conocer los datos de calculamiento de rutas.
4. Los **datos que se envían entre puntos de atención al cliente y servidor** pueden ser vulnerados en integridad y confidencialidad dado que un actor externo que no tiene permisos de acceso podría modificar los datos o la información puede ser disponible para personas no autorizadas.

**B Propuesta de soluciones**

Para el **manejo de los datos contables** se desearía que la intranet contara con protección a los datos usando función de hash a las contraseñas. De esta forma, la información confidencial como contraseñas se cifran y los actores externos no podrán acceder a las cuentas de los usuarios dado que no sabrían las contraseñas de esas cuentas. Esto solucionaría el problema de autorización de los datos contables que solo serán adquiridos por usuarios autorizados y que no pueden ser suplantados.

Para la **información de rastreo** se quiere verificar qué estación envía la información y que sea consistente. Se puede cifrar la información con llave privada del emisor y el servidor usa la llave pública. De esta forma se garantiza el no repudio de los datos.

Para los **datos de manejo de ordenes**  puede usar una llave simétrica que solo la empresa la tenga. De esta forma cuando guarda la información en los servidores, cifra esa información y al momento de requerirla vuelve a usar la llave para descifrarla. Esto evita la no confidencialidad de los datos.

Para **los datos que se envían entre cliente y servidor** se puede usar cifrado asimétrico para comprobar que el receptor del archivo sea el deseado y usar función de hash a los datos para comprobar que los datos no hayan sido modificados. Esto soluciona integridad y confidencialidad.