

Análisis de riesgos Empresa transporte

Fecha

Autores

19/09/2024

Sandra González y Gonzalo Celaya

Identificación

Activos críticos del sistema:

- **Datos de clientes:** Información de contacto, datos de pago y acuerdos comerciales con clientes corporativos o individuales que solicitan servicios de transporte.
- **Datos de transportistas y camiones:** Información sobre la flota de vehículos, como matrículas, mantenimiento, ubicaciones GPS, y datos personales de los conductores.
- **Catálogo de rutas:** Rutas y trayectos logísticos utilizados para la planificación del transporte. Información crítica, especialmente en servicios de carga sensible o de alto valor.
- **Solicitudes de servicio:** Datos sobre la carga, tipo de servicio solicitado, destino, tiempos de entrega, etc.
- **Facturación y pagos:** Información financiera tanto de los clientes como de la propia empresa para gestionar cobros y pagos.
- **Sistema de gestión de flota y logística:** Control del estado de los vehículos, planificación de rutas y asignación de camiones a servicios específicos.

Vulnerabilidades

Principales vulnerabilidades del sistema:

- **Autenticación débil para transportistas y operadores:** Un sistema de autenticación sin controles robustos podría permitir que atacantes accedan a información operativa crucial, como rutas o detalles de la carga.
- **Cifrado insuficiente de datos en tiempo real (GPS y telemetría):** Los datos de ubicación y condiciones de los vehículos (como GPS y estado de la carga) deben estar cifrados para evitar que terceros intercepten información crítica.
- **Inyección de código en formularios de solicitud de servicio:** Si no se validan adecuadamente las solicitudes de transporte, se corre el riesgo de ataques de inyección de código (SQL, XSS), permitiendo la manipulación de la base de datos con información de rutas o facturación.
- **Gestión inadecuada de parches en sistemas de logística:** Las plataformas de gestión de flota y los sistemas GPS pueden contener vulnerabilidades que, si no se actualizan regularmente, podrían ser explotadas para obtener control sobre las operaciones.
- **Protección insuficiente de API utilizadas para integrar sistemas GPS y ERP:** Si las API de la página web que integran datos de ubicación en tiempo real con los sistemas ERP (gestión de recursos empresariales) no están aseguradas, podrían ser vulnerables a ataques de interceptación.
- **Mala configuración de sistemas de alertas y notificaciones:** Si las notificaciones que alertan sobre el estado de la flota, incidentes o cambios en las rutas no están bien protegidas, podrían generar información errónea que afecte la operación logística.



Amenazas

Amenaza	Descripción	Activos afectados	Impacto
Interceptación de datos GPS	Interceptación de los datos de geolocalización de los camiones que permiten seguir sus rutas y planificar robos.	<ul style="list-style-type: none"> • Información de rutas • Ubicación de camiones y transportistas • Seguridad de las cargas 	Alto
Ataques a la cadena de suministro	Ataques que afectan la planificación y ejecución de las rutas logísticas, retrasando entregas o desviando camiones.	<ul style="list-style-type: none"> • Datos de planificación logística • Catálogo de rutas • Sistema de gestión de flota 	Alto
Acceso no autorizado a la planificación de rutas	Acceso no autorizado a los sistemas que gestionan las rutas, permitiendo modificar, desviar o cancelar transportes.	<ul style="list-style-type: none"> • Sistema de planificación de rutas • Información de transportistas • Datos de clientes 	Crítico
Robo de datos de clientes	Exposición de información sensible sobre clientes, contratos y acuerdos comerciales.	<ul style="list-style-type: none"> • Información de clientes • Facturación • Acuerdos y contratos 	Alto
Manipulación de la facturación	Modificación o alteración de las facturas y pagos, generando fraude financiero.	<ul style="list-style-type: none"> • Sistema de facturación • Información financiera de clientes • Datos de cobros y pagos 	Alto
Amenazas internas (empleados/transportistas)	Abuso de acceso autorizado por parte de empleados o transportistas para manipular datos o colaborar en robos.	<ul style="list-style-type: none"> • Datos de rutas y carga • Sistema de gestión de flota • Información financiera 	Medio

Evaluación de riesgo

Riesgo	Prob.	Riesgo	Acción
Interceptación de datos GPS	Alta	Crítico	Implementar cifrado en tiempo real para datos GPS y comunicaciones con los camiones.
Ataques a la cadena de suministro	Media	Alto	Aplicar autenticación multifactor (MFA) en los sistemas de planificación de rutas y control logístico.
Acceso no autorizado a la planificación de rutas	Media	Alto	Limitar el acceso a la planificación mediante políticas de control de roles y permisos estrictos.
Robo de datos de clientes	Media	Alto	Cifrar los datos de clientes en reposo y en tránsito, y aplicar controles de acceso adecuados.
Manipulación de la facturación	Baja	Alto	Implementar auditorías regulares en el sistema de facturación y el control de cambios.
Amenazas internas (empleados/transportistas)	Baja	Moderado	Monitorear actividades de usuarios internos y aplicar políticas de control de acceso granular.

Medidas de mitigación

Interceptación de datos GPS

- **Cifrado en tiempo real de datos GPS:** Asegurar que todos los datos de localización de los camiones sean cifrados utilizando protocolos como TLS para que no puedan ser interceptados por terceros malintencionados.
- **Autenticación robusta en sistemas de localización:** Aplicar medidas de autenticación adicionales, como autenticación multifactor, para evitar accesos no autorizados a los sistemas de seguimiento GPS.

Ataques a la cadena de suministro

- **Autenticación multifactor (MFA):** Implementar MFA para todos los usuarios que accedan a los sistemas de planificación de rutas y logística. Esto evita que actores no autorizados manipulen la cadena de suministro.
- **Supervisión continua de los sistemas de planificación:** Implementar sistemas de monitoreo que detecten cualquier actividad anómala en los procesos de planificación y ejecución de rutas.

Acceso no autorizado a la planificación de rutas

- **Roles y permisos estrictos:** Limitar el acceso a los sistemas de planificación de rutas solo a aquellos empleados o transportistas que lo requieran para sus funciones específicas.
- **Monitoreo de acceso:** Implementar monitoreo y auditorías periódicas para revisar los accesos y las modificaciones en la planificación de rutas. Esto previene accesos indebidos y permite una rápida detección de anomalías.

Robo de datos de clientes

- **Cifrado de datos en reposo y en tránsito:** Proteger los datos de los clientes mediante el uso de cifrado AES en bases de datos y SSL/TLS para las comunicaciones. De esta manera, incluso si los datos son interceptados, no podrán ser leídos sin la clave de cifrado.
- **Control de acceso basado en roles (RBAC):** Restringir el acceso a los datos sensibles de los clientes solo a aquellos empleados que lo necesiten para su trabajo, minimizando las oportunidades de exfiltración de datos.

Manipulación de la facturación

- **Auditorías periódicas de sistemas de facturación:** Realizar auditorías automáticas y manuales del sistema de facturación para detectar y corregir cualquier intento de manipulación o fraude.
- **Control de versiones y registros de auditoría:** Implementar un control estricto de versiones de las facturas y un registro detallado de quién ha accedido o modificado datos financieros. Esto permitirá rastrear cambios no autorizados.

Amenazas internas (empleados y transportistas)

- **Monitoreo de actividades de usuarios internos:** Implementar un sistema que registre y audite la actividad de los empleados y transportistas dentro de los sistemas críticos, como los de planificación de rutas y gestión de flotas, para identificar posibles abusos de acceso.
- **Política de acceso con privilegios mínimos:** Asegurarse de que cada usuario tenga acceso únicamente a la información necesaria para su rol, minimizando el riesgo de uso indebido de los datos o los sistemas.

Confidencialidad,
Integridad y
Disponibilidad


Confidencialidad

Protección de información sensible. Los datos que requieren de mayor protección incluyen información personal y financiera, rutas logísticas, geolocalización de vehículos y detalles de las cargas transportadas.

- **Riesgos:**

- **Intercepción de datos GPS:** Los datos de ubicación de los camiones en tiempo real podrían ser interceptados, revelando información crítica sobre las rutas y ubicaciones de vehículos que transportan mercancías valiosas.
- **Robo de datos de clientes:** La filtración de información sensible de clientes, como contratos o datos financieros, puede afectar la confianza y la reputación de la empresa.

- **Medidas de Mitigación:**

- **Cifrado en tiempo real** de los datos GPS y de toda la información sensible relacionada con clientes y rutas, tanto en tránsito como en reposo.
 - **Autenticación robusta y control de acceso** a la información crítica para garantizar que solo personal autorizado acceda a los datos sensibles.
- 

Integridad


Exactitud y confiabilidad de los datos, asegurando que no se modifiquen de manera no autorizada.

- **Impacto del Riesgo:** Las vulnerabilidades como la inyección SQL (SQLi) o la manipulación

- Riesgos:**

- **Manipulación de la planificación de rutas:** Un acceso no autorizado a los sistemas de planificación de rutas podría permitir la modificación de trayectos, desvíos o alteraciones en el transporte, afectando las entregas y comprometiendo la seguridad de la carga.
- **Manipulación de la facturación:** Alteraciones en las facturas o los registros de pago podrían llevar a fraude financiero y discrepancias en los balances.

- **Medidas de Mitigación:**

- **Control estricto de roles y permisos** para evitar que usuarios no autorizados puedan modificar la planificación de rutas o los registros de facturación.
 - **Auditorías periódicas** y el uso de **registros de auditoría** para asegurar que cualquier cambio en los sistemas de planificación o facturación esté adecuadamente registrado y sea rastreable.
- 

Disponibilidad

Capacidad de que los sistemas logísticos y de la gestión de la flota estén siempre operativos.

- **Riesgos:**

- **Ataques de denegación de servicio (DDoS):** Estos ataques pueden dejar fuera de línea la página web o los sistemas de gestión de flota, imposibilitando la gestión eficiente de los vehículos y las entregas.
- **Fallas en los servidores de planificación logística:** Si los sistemas de planificación de rutas o asignación de camiones no están disponibles, se pueden generar retrasos en las entregas y pérdidas operativas.

- **Medidas de Mitigación:**

- **Protección contra DDoS** mediante servicios de mitigación especializados y balanceo de carga, garantizando que los sistemas web y de gestión de flota puedan resistir grandes volúmenes de tráfico malicioso.
- **Copias de seguridad periódicas** y planes de recuperación ante desastres para asegurar que, en caso de una interrupción, los datos y sistemas críticos puedan ser restaurados rápidamente.