Buenas prácticas para la gestión de la ciberseguridad en el ámbito de la telemática

GEOTAB®

El valor de los datos telemáticos

La telemática genera una gran cantidad de datos, incluyendo una historia detallada de las operaciones y las actividades del conductor y del vehículo. Este tipo de datos resulta extremadamente útil en una organización, ya que permiten supervisar los costes de combustible y de mantenimiento, aumentar la productividad y la seguridad y minimizar los riesgos. El uso de la telemática para reconstruir un accidente o para comparar información puede generar incluso más datos.

Proteger esos datos es de gran importancia. Si alguien accediera a esos datos malintencionadamente, podría haber consecuencias graves que podrían incluso poner en peligro las cuentas de los clientes, los horarios, los envíos, la ubicación de los activos e información personal. Los delitos cibernéticos se cometen porque alguien considera que puede obtener algo de valor de lo datos, ya sea al recopilar los nombres de usuario y contraseñas, los números de las tarjetas de crédito, los números de la seguridad social o, como veremos en estas páginas, datos telemáticos.

Por eso, independientemente de que sea el propietario de un pequeño negocio, un gestor de flotas, desarrollador, responsable de los sistemas tecnológicos o director ejecutivo de una empresa, es muy importante comprender cómo se gestionan y protegen los datos telemáticos.

¿Qué aprenderá?

En esta guía aprenderá lo siguiente:

+ La estructura del ecosistema telemático
+ La manera en que Geotab protege los datos telemáticos en cada nivel
+ Las mejores prácticas para la ciberseguridad telemática
+ Cuestiones clave para preguntar a su proveedor de tecnología telemática acerca de la seguridad de los datos

Visión general del ecosistema telemático

La telemática de plataforma abierta conecta múltiples dispositivos del Internet de las Cosas al vehículo a través de un sistema de comunicaciones centralizado del dispositivo GO de Geotab. Cada vez más, un mayor número de dispositivos de terceros se pueden integrar con las soluciones telemáticas, entre las que se incluyen soluciones disponibles en el Marketplace de Geotab:

+ Dispositivos Bluetooth
+ Sensores de temperatura
+ Sensores de la presión de los neumáticos
+ Avisos verbales para el interior del vehículo
+ Sistemas para evitar colisiones
+ Cámaras

El ecosistema telemático incluye tanto el hardware como el software responsable de recoger y analizar los datos del vehículo.

El Ecosistema Telemático

Área	Descripción
Dispositivo telemático GO de Geotab Dispositivo telemático reforzado GO RUGGED	El dispositivo GO de Geotab es un pequeño dispositivo telemático equipado con un módulo GPS y un acelerómetro de calibración automática que se conecta al puerto de diagnóstico del vehículo. El dispositivo recopila datos sobre la posición del vehículo, frenados bruscos, conducción brusca, el uso de los cinturones de seguridad, el consumo de combustible, el odómetro, los códigos de error del vehículo, el voltaje de la batería, la temperatura del aire y otros datos sobre el motor. El dispositivo envía sus datos al entorno almacenado en la nube de MyGeotab para procesarlos y analizarlos.
Software de gestión de flotas MyGeotab	Un software basado en la web, flexible y escalable que se utiliza para gestionar flotas, analizar los datos telemáticos y visualizar reportes. Las características clave de este software incluyen seguimiento de vehículos por GPS, elaboración avanzada de reportes, gestión del comportamiento del conductor, reportes sobre datos del motor, optimización de rutas, salud y mantenimiento del motor, reconstrucción de colisiones, integración de datos abiertos y mapeo personalizado.
Extensores de entrada/salida (IOX)	Son elementos de hardware de terceros que se conectan al puerto de extensión del dispositivo telemático de Geotab para realizar tareas específicas y transmitir información a y de MyGeotab. **Ejemplos:** identificación del conductor a través de NFC, avisos verbales de GO TALK en el vehículo, supervisión del esparcidor de sal y arena, y comunicación del dispositivo a través de la red de satélites Iridium para los trabajadores que trabajan en lugares remotos.
Soluciones del Marketplace	Tienda online de soluciones de gestión de flotas que se integran con la plataforma abierta de telemática de Geotab. En el Marketplace encontrará Add-Ins de software, accesorios y Add-Ons de hardware, aplicaciones móviles, soluciones de software generales y reportes personalizados.
Kit de desarrollo de software (SDK) Interfaces de programación de aplicaciones (API)	El kit de desarrollo de software (SDK) y las interfaces de programación de aplicaciones (API) son un conjunto de herramientas para automatizar tareas, construir Add-Ons de hardware de terceros para el dispositivo Geotab GO e integrar sistemas empresariales, entre ellos de contabilidad, nóminas, CRM, mantenimiento, planificación de rutas, gestión de riesgos y cumplimiento de normas de seguridad.

Buenas prácticas para la ciberseguridad telemática

Cada vez más son más las empresas que deciden dar el salto hacia sistemas basados en software y/o hacia la nube. A medida que esto sucede, la seguridad de los datos telemáticos se convierte en un reto cada vez mayor. Los sistemas telemáticos son expansivos y tienen múltiples niveles: son una combinación de hardware físico, sistemas de radio, servidores de software y agentes humanos. Al tener tantos componentes en juego, son muchas las posibles amenazas[1,2] entre las que se pueden incluir el robo, interferencias del GPS, sniffing móvil, manipulación de firmware, exploits de software y suplantación de identidad (phishing).

Estrategias generales para la ciberseguridad

Para proteger los datos telemáticos es necesario adoptar un enfoque integral y proactivo. La integridad de los sistemas se basa en el mantenimiento de muchos subsistemas, cada uno de los cuales presenta distintas vulnerabilidades posibles. Por eso, además de contar con políticas y procesos sólidos, la mejor manera de proteger los datos y de crear una barrera ante ataques malintencionados es crear una cultura de seguridad en la organización.

En general, la seguridad telemática se puede fortalecer con estos principios que conforman la seguridad del Internet de las Cosas:[3,4]

Liderazgo

Establecer un equipo dedicado de especialistas en seguridad y gestión que crean en la importancia de la seguridad.

Diseño

Implementar buenas prácticas de seguridad en el desarrollo de productos y software.

Políticas

Establecer políticas integrales y transparentes sobre seguridad y privacidad.

Educación

Impartir entrenamiento o formación frecuente para empleados, socios y usuarios finales acerca de las políticas y los procedimientos de seguridad.

Las 15 recomendaciones para tener una plataforma telemática resistente

La necesidad de una mayor seguridad para el vehículo conectado se impone cada vez más. El FBI recomienda que “los propietarios de vehículos comprueben las políticas de seguridad y privacidad de los fabricantes de dispositivos de terceros y proveedores de servicios, y que no deberían conectar ningún dispositivo desconocido o no confiable al puerto OBD II”.[5] De modo parecido, la Asociación de Gestión de Flotas, NAFA recomienda que “los gestores de flotas tengan instauradas políticas para garantizar que en el puerto solo se conectan dispositivos seguros”.[6]

Geotab propone las 15 recomendaciones de seguridad siguientes para construir una plataforma telemática resistente a las amenazas cibernéticas.[7]

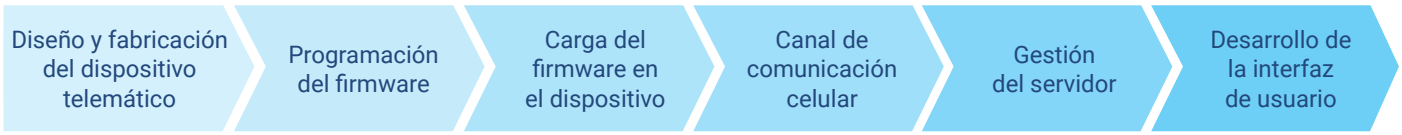
1. Implementar la transferencia segura de datos.
2. Firmar digitalmente las actualizaciones.
3. Habilitar la protección del código de hardware.
4. Ser consciente de que el código es público, para no depender de secretos.
5. Utilizar números aleatorios criptográficamente fuertes que no puedan ser sometidos a prácticas de ingeniería inversa.
6. Individualizar datos de seguridad críticos.
7. Utilizar distintas claves para roles distintos.
8. Supervisar los metadatos para detectar intentos de piratería.
9. No olvidar deshabilitar características para depurar errores.
10. Realizar auditorías de terceros.
11. Limitar el acceso al servidor.
12. Aplicar prácticas de diseño seguras.
13. Implementar apoyo para las actualizaciones de software o firmware.
14. Verificar y comprobar.
15. Desarrollar una cultura de seguridad.

Seguridad de la plataforma telemática de Geotab

Geotab toma la seguridad de los datos con rigurosidad, siguiendo el principio de mejora continua. A fin de proteger a nuestros clientes y partners, Geotab revisa, mejora y valida constantemente los mecanismos y procesos de seguridad con la intención de que los sistemas sigan siendo resistentes a intrusiones externas. Geotab proporciona a sus clientes documentación detallada sobre las medidas técnicas y organizativas sobre seguridad de datos implementadas en todo nuestro ecosistema. Además, colabora con los agentes principales para seguir progresando en la seguridad de toda la industria.

Como proveedor telemático integral, Geotab participa directamente en cada una de las etapas del ecosistema telemático.

Fortaleza a través de la integración vertical



La seguridad de la plataforma de Geotab está diseñada para ofrecer una protección integral de sus datos. Las principales implementaciones incluyen:

+ Las interfaces del dispositivo GO y la red utilizan autenticación, cifrado y verificación de la integridad de los mensajes para garantizar que otras partes malintencionadas puedan leer o falsificar los datos telemáticos.
+ Las actualizaciones over-the-air (OTA) utilizan firmware firmado digitalmente para verificar que las actualizaciones provengan de una fuente de confianza.
+ Geotab utiliza a expertos independientes y externos para validar la totalidad de la plataforma.

A continuación se presenta información adicional sobre la manera en que se consigue la seguridad del sistema telemático.

Seguridad en el diseño y la fabricación

Los módulos microelectrónicos de los dispositivos Geotab GO se fabrican en distintas instalaciones en todo el mundo. Una vez fabricados, los distintos componentes regresan a las instalaciones de Geotab, donde los empleados de Geotab finalizan el ensamblaje del hardware del dispositivo GO. Se comprueban los componentes electrónicos de cada uno de los dispositivos y, a continuación, se preparan para realizar la programación del firmware.

Geotab no compra el hardware del dispositivo a ninguna entidad y tiene pleno control de los procesos de diseño, fabricación, ensamblaje y calidad, lo que nos permite responder con rapidez y eficacia a nivel interno ante los defectos de fabricación o posibles vulnerabilidades de software, sin tener que depender de ninguna otra parte.

Seguridad del firmware

El firmware es un software especializado que controla los múltiples módulos electrónicos que hay en un dispositivo telemático. Permite que el dispositivo se comunique con el motor de un vehículo y los sistemas auxiliares para poder recibir las coordenadas GPS procedentes de satélites y también para coordinar la transferencia de datos utilizando redes celulares.

El dispositivo telemático está conectado al complejo sistema interconectado del vehículo, por lo que el firmware del dispositivo se convierte en una parte excepcionalmente importante del sistema conectado debido al control que ejerce sobre los datos obtenidos del vehículo.

Por eso, es importante actualizar de manera continua el firmware de los dispositivos telemáticos para añadir prestaciones y para poder detectar posibles vulnerabilidades en su código. Las actualizaciones se producen automáticamente sin que el usuario tenga que hacer nada, ya que se reciben over-the-air, al igual que el proceso de instalación.

Estas actualizaciones son sencillas y muy convenientes. Aún así, existe la posibilidad de ataques para intentar sustituir el firmware de un dispositivo telemático con firmware malintencionado. Si dicho ataque sucediera, la persona que comete el ataque tendría pleno control sobre el dispositivo telemático.

A fin de evitar ataques de este tipo, se deben utilizar los siguientes métodos para mantener la seguridad del dispositivo:

+ Controlar la instalación del firmware en el dispositivo en la fase de fabricación.
+ Firmar digitalmente las actualizaciones over-the-air para verificar que las actualizaciones proceden de una fuente fiable.

Si no se cumplen ambos pasos para verificar que la actualización de software es auténtica, resulta imposible saber si es usted quien tiene el control del dispositivo o si, por el contrario, lo tiene un tercero con malas intenciones e interesado en obtener sus datos.

Transferencia segura de datos

El dispositivo telemático envía datos desde el vehículo al servidor central a través de una conexión móvil. Aunque varía según el territorio, el proveedor y la infraestructura, la comunicación móvil se suele realizar utilizando redes 2G, 3G y LTE. Todas estas redes pueden tener sus propias vulnerabilidades.[8]

Se puede establecer un canal de comunicación seguro utilizando el cifrado (también conocido como encriptación). El cifrado es un proceso mediante el cual se codifica el mensaje de modo que solo el remitente y el receptor pueden visualizar el contenido del mensaje. Así pues, un tercero (por ejemplo, alguien que quiera cometer un ataque) vería este mensaje codificado como una mera sucesión de símbolos sin sentido. El receptor a quien se dirigía el mensaje puede convertir este conjunto de símbolos en información inteligible mediante el uso de una clave.

De ese modo, la seguridad de un canal normalmente vulnerable, como una red móvil, se puede lograr mediante el cifrado de los mensajes que se envíen de un dispositivo telemático a un servidor destinatario. Debido a sus propiedades matemáticas, un cifrado potente no se puede descifrar fácilmente, ni siquiera en los PC más potentes. Los dispositivos de Geotab utilizan uno de los cifrados más avanzados del sector.

La seguridad en la nube

Los dispositivos telemáticos transmiten sus datos a servidores de almacenaje y procesamiento. Se podría pensar en estos servidores como si fueran cajas fuertes que contienen información valiosa. Para proteger los servidores, se puede restringir el acceso físico y que solamente personas autorizadas tengan acceso a ellos. Por otro lado, los datos almacenados en los servidores se pueden proteger manteniendo la seguridad del entorno en la nube. Para ello, se deben utilizar cortafuegos (firewalls) estándares de la industria, controles de acceso y contar con una supervisión de la actividad.

Sin embargo, resulta crucial comprender que incluso los sistemas más seguros distan de ser perfectos. En el caso de que la seguridad del sistema se vea comprometida, es importante poder mitigar el daño causado por un acceso no autorizado.

Esta mitigación consiste en minimizar el posible impacto de una amenaza. En la nube, es posible lograr una mitigación eficaz de una manera sencilla: no se deben almacenar nunca las contraseñas del usuario para evitar su robo ante posibles ataques. Este proceso se conoce como hash y sal (hashing y salting) de una contraseña, es decir, almacenar un valor hash y sal de una contraseña en vez de la propia contraseña. Este proceso ralentiza la velocidad con la que el atacante puede obtener datos valiosos del usuario a través de la nube si logra acceder de manera no autorizada. De esta manera, se gana un tiempo muy importante que permite responder al compromiso de seguridad y atenuar el daño.

El hashing y salting prolongan la metáfora de la caja fuerte: si un ladrón accede a la caja fuerte de un banco, no tendrá acceso directo a todos los tesoros que allí se almacenan, sino que para poder acceder a ellos tendría que ir asaltando cada una de las cajas fuertes para poder robar los objetos de valor que se encuentran en su interior.

Cultura corporativa de seguridad

La seguridad de los datos consiste en una práctica, más que en un acto. A medida que la tecnología avanza y la complejidad de los sistemas aumenta, surgirán nuevas amenazas de seguridad. Una organización que se tome en serio la seguridad dedicará esfuerzos constantes a afrontar estos problemas de seguridad, y para ello actualizará sus sistemas, ofrecerá formación a sus empleados, mejorará sus procesos y se dedicará a encontrar vulnerabilidades de los sistemas.

El núcleo de todo sistema telemático lo conforman el equipo de ingenieros y personal de apoyo que se encarga de que todo funcione sin problemas. Las organizaciones deberían tener en cuenta que un empleado puede llegar a actuar en contra de los intereses de la empresa, ya sea porque filtra datos a la competencia a cambio de algo o porque se producen errores accidentales.

Por eso, resulta esencial que las organizaciones se mantengan siempre alerta a todos los niveles. Esto se puede conseguir a través del control y supervisión de los privilegios de acceso, llevando un registro de las operaciones importantes y asegurándose de que todos los empleados conocen los riesgos que implican sus acciones. Una cultura de seguridad sólida debe inspirar confianza en los empleados para que puedan responder ante amenazas de seguridad, pero sin llegar a crear ansiedad por los ataques que podrían llegar a suceder o no.

Una manera de inspirar esta confianza en temas de seguridad en la organización es exponer los sistemas a pruebas de penetración (conocidas también como pen tests). Estas pruebas consisten en intentos de pirateo autorizados que realiza una empresa externa especializada en seguridad informática. En estas pruebas, la empresa dedicada a temas de seguridad intenta encontrar las vulnerabilidades del hardware y el software. Sin embargo, a diferencia de un hacker, no se aprovecha de estas vulnerabilidades, sino que documenta la metodología utilizada en el ataque y comunica los resultados a la empresa que le ha contratado. Una vez que se dispone de estos resultados, es necesario tomar medidas, ya sea arreglando las brechas de seguridad o cambiando los procedimientos internos, antes de que atacantes malintencionados se aprovechen de esas mismas vulnerabilidades.

Para concluir, es importante recalcar que la seguridad de los datos es un esfuerzo constante que toda la empresa debe realizar para salvaguardar los datos de todos los usuarios.

Cinco preguntas clave que debe plantear a su proveedor de telemática

La seguridad es un tema complejo que afecta a la integridad del sistema telemático. No basta con preguntarse si nuestros datos están seguros, sino que debemos plantearnos preguntas más profundas, teniendo en cuenta que trabajamos con datos valiosos. Es importante llevar a cabo estrategias y modos de aplicación específicos que conforman la base de los estándares de seguridad modernos.

A continuación, proponemos una serie de preguntas sobre la seguridad de los datos telemáticos que deben servir como pilares básicos a la hora de tratar y establecer relaciones con los proveedores de sistemas telemáticos.

1 ¿Quién se encarga de la fabricación del hardware de los dispositivos telemáticos? ¿El dispositivo será el mismo para toda mi flota?

Por qué es importante esta pregunta: Si su fabricante de telemática no fabrica su propio hardware, es posible que no tenga un buen conocimiento de la seguridad del hardware. Asimismo, si su proveedor no tiene control directo sobre la seguridad del software y el hardware, es posible que necesite más tiempo para responder a las amenazas o vulnerabilidades de seguridad, ya que tendrán que coordinarse con terceros.

Además, los dispositivos electrónicos se actualizan con frecuencia. Los distintos modelos de hardware pueden presentar distintos conjuntos de vulnerabilidades para cada modelo; es decir, hará falta trabajar más para remediar estas brechas de seguridad a lo largo de la línea de producción. Al haber más variedades de hardware, los ingenieros se enfrentan a una exigencia mayor para mantener y solucionar las brechas de seguridad. De este modo, es posible que los recursos no se distribuyan de manera uniforme y que la atención prestada varíe debido a la complejidad del producto, lo que puede provocar que existan omisiones o no se detecten vulnerabilidades. Los fabricantes son los responsables de la seguridad durante todo el ciclo de vida de un producto.

2 ¿Cifra los datos tal como se envían por medio de la red móvil?

Por qué es importante esta pregunta: No se debe confiar exclusivamente en los operadores de tecnología móvil para garantizar el envío seguro de los datos telemáticos over-the-air. Es importante que sus proveedores de servicios telemáticos adopten medidas adicionales para cifrar sus datos, de modo que aunque el canal de comunicación celular se vea amenazado, los datos no lo estén.

3 ¿El firmware está firmado para evitar que alguien externo cambie el código del dispositivo?

Por qué es importante esta pregunta: El firmware es el cerebro del dispositivo, el que decide dónde se envían los datos, qué datos se obtienen y cómo se almacenan. Si se instalara firmware malintencionado en su dispositivo, ya no sería posible saber dónde se envían los datos ni qué se hace con ellos. Su proveedor telemático debería firmar todas las actualizaciones de firmware con una firma digital que indique que la actualización procede de una fuente fiable.

4 ¿Dispone de documentación sobre seguridad acerca de su hardware, sus servidores, la transmisión de datos y también las políticas para los empleados?

Por qué es importante esta pregunta: La documentación sobre seguridad demuestra un compromiso de base con la cultura de seguridad. El proveedor de telemática debería ser capaz de proporcionar información sobre las medidas de seguridad que utiliza, así como sobre sus estrategias de mitigación y recuperación ante desastres en el caso de que sucediera algo inesperado.

Existe un documento orientativo sobre los procesos de seguridad (Medidas técnicas y organizativas sobre seguridad de datos, en inglés) que le puede ayudar a comprender lo que sucede con sus datos.

5 Si sus servidores estuvieran en peligro, ¿qué tipo de estrategia de mitigación utilizaría para proteger la información de las cuentas de sus usuarios?

Por qué es importante esta pregunta: Si se produce una brecha de seguridad, en el sistema debería haber la mínima información personal posible. Las contraseñas jamás se deben guardar directamente en el sistema de su proveedor de telemática, por el contrario, las contraseñas se deben transformar y fortalecer utilizando hash y a través del salting.

Resumen

No debe pasar por alto la seguridad de sus datos telemáticos. Al igual que sucede con cualquier tipo de dato empresarial importante, los datos telemáticos, deben ser protegidos con mecanismos y procesos de seguridad completos que hay que revisar y actualizar constantemente. Resulta esencial seguir las mejores prácticas de la industria.

Dicho esto, la seguridad cibernética es una responsabilidad compartida, y todos podemos desempeñar un papel importante a la hora de mantener seguros nuestros sistemas. Obtener información y hacer preguntas es un gran primer paso para realizar una gestión eficaz de la ciberseguridad (o seguridad cibernética).

Para obtener más información sobre seguridad telemática, visite www.geotab.com/es/security

Acerca de Geotab

Geotab conecta de forma segura vehículos a Internet, proporcionando análisis avanzados para la gestión de flotas. La plataforma abierta y el Marketplace permiten a las pequeñas y grandes empresas automatizar procesos mediante la integración de datos de vehículos con otros datos de la compañía. El dispositivo de GO actúa como un hub de IoT para el vehículo permitiendo la conectividad de funcionalidades adicionales a través de complementos IOX. Geotab procesa millones de puntos de datos al día que son aprovechados para análisis de big data y aprendizaje automático (machine learning) para mejorar la productividad, optimizar las flotas a través de la reducción del consumo de combustible, mejorar la seguridad del conductor y lograr un mayor cumplimiento de la regulación. Los productos de Geotab se pueden adquirir en cualquier país del mundo a través de una red de distribuidores autorizados.

Para más información, visite www.geotab.com/es o síganos en @GEOTAB y en LinkedIn.

Referencias

1. S. Kilcarr, “Telematics hacking: Three things you need to know,” Sep. 3, 2015. Retrieved from: http://fleetowner.com/technology/telematics-hacking-three-things-you-need-know
2. H. Williams, “Top five biggest threats to IoT security,” Oct. 24, 2016. Retrieved from: http://www.cbronline.com/news/cybersecurity/breaches/top-five-biggest-threats-iot-security/
3. M. Turner, “How to secure the internet of things,” June 2015. Retrieved from: http://www.computerweekly.com/opinion/How-to-secure-the-internet-of-things
4. Accenture, “Securing the Internet of Things: Executive Summary,” 2015. Retrieved from: https://www.accenture.com/t00010101T000000__w__/jp-ja/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents22/Accenture-Security-Call-to-Action-IoT-ExecSummary-FINAL.pdf
5. Federal Bureau of Investigation, “Alert Number I-031716-PSA: Motor Vehicles Increasingly Vulnerable to Remote Exploits,” Mar. 17, 2016. [Online] Available: https://www.ic3.gov/media/2016/160317.aspx.
6. NAFA Fleet Management Association, “Fleet Management and the Connected Vehicle,” Oct. 2016. [Online] Available: www.nafa.org/download.php?f=832
7. A. Sukhov, “15 Security Recommendations for Building a Telematics Platform Resilient to Cyber Threats,” Nov. 14, 2016. Retrieved from: https://www.geotab.com/blog/telematics-cybersecurity-recommendations/
8. D. Perez and J. Pico, “A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications,” 2011. Retrieved from: http://media.blackhat.com/bh-dc-11/Perez-Pico/BlackHat_DC_2011_Perez-Pico_Mobile_Attacks-wp.pdf

GEOTAB®

www.geotab.com/es