CONECTIVIDAD:

¿UNA BRECHA EN LA SEGURIDAD DE LOS VEHÍCULOS?

La conectividad de los vehículos está generando grandes oportunidades al sector de la automoción, hasta el punto de que ya no entendemos la movilidad sin conectividad, una movilidad que avanza con paso firme en último término hacia la automatización total de la conducción. Las posibilidades son casi infinitas...pero ¿qué pasaría si alguien fuera capaz de actuar sobre un determinado sistema de nuestro vehículo, inutilizándolo o provocando una lectura errónea de ese sensor, cámara o radar?

A día de hoy, alcanzar el nivel máximo de automatización, es decir, aquel en el que no es necesaria la participación de una persona a bordo del vehículo está aún lejos. Pero los vehículos, en especial los vehículos industriales, han recorrido un enorme camino en esa dirección, implementando sofisticados sistemas telemáticos, para "controlar" una enorme cantidad de parámetros del vehículo de forma remota, o sistemas de ayudas a la conducción que automatizan muchas acciones, gracias a complejos ecosistemas de radares, sensores, cámaras, etc. Sólo en un camión de última generación podemos encontrarnos más de 200 sensores que miden todo tipo de parámetros, desde la presión de los neumáticos, al sistema de frenado activo, gracias al cual podemos programar la distancia mínima a la que queremos que nuestro camión reaccione ante un objeto.

Pero...¿y si fuera posible que alguien pudiera acceder de manera remota a estos sensores?

Este peligro es real. Está presente allá donde hay conexiones e intercambio de datos que se pueden "hackear"..y el mundo de la automoción, también el del vehículo industrial no está exento. Es por eso que conviene empezar a manejar el término "Ciberseguridad" aplicado a los vehículos.

Azucena Hernández, CEO de la empresa Eurocybcar dedicada a realizar las pruebas de los vehículos que certifican si son "ciberseguros", define un ciberataque a un vehículo como "el intento, por parte de un cracker, de acceder a los sistemas del vehículo para manipular, modificar, robar o eliminar información que gestiona o almacena el vehículo, con la intención de poner en riesgo la privacidad o la vida de los usuarios y pasajeros que viajan a bordo…" Por esa razón, un vehículo se debe proteger de la misma forma o incluso más que un móvil, un ordenador portátil, una empresa…

En este sentido, los vehículos que circulan por nuestras carreteras, como mínimo, disponen de Bluetooth, USB, WiFi, eCall, GPS… generadores constantes de intercambio de información y datos que se transmiten. "Toda esa tecno-

> El futuro inmediato de la movilidad se dirige hacia vehículos eléctricos y autónomos hiperconectados con otros vehículos, con las infraestructuras, con la nube… "por lo que los ataques que pueden sufrir seguirán aumentando de manera drástica si no se toman medidas".

Los vehículos que circulan por nuestras carreteras, como mínimo, disponen de Bluetooth, USB, WiFi, eCall, GPS… generadores constantes de intercambio de información y datos que se transmiten.

logía-asegura Hernández- si no es cibersegura, son puertas de acceso que pueden ser utilizadas por un cracker… incluso si los sensores que incorporan los vehículos no están suficientemente protegidos, pueden ser manipulados, impidiendo que cumplan su función de forma correcta o que la información que transmiten provoquen que el vehículo se comporte de forma peligrosa -como por ejemplo, circular a 120 km/hora en una vía con limitación de velocidad de 20km/hora-".

No es ciencia ficción

Aunque a primera vista pueda parecer ciencia ficción, lo cierto es que desde el año 2012 está siendo una realidad: "se han robado coches de forma remota, se han "secuestrado" vehículos para pedir una recompensa en bitcoins, se ha accedido a información personal del conductor a través del sistema Bluetooth mientras conducía, se ha bloqueado el acceso al interior del vehículo, se han llamado coches a revisión por un fallo de ciberseguridad…", afirma la responsable de esta empresa que recientemente junto con Centro Zaragoza han firmado un convenio de colaboración, uniendo sus respectivas áreas de conocimiento, para trabajar en favor de la mejora de la seguridad vial y la ciberseguridad de los vehículos.

Un ejemplo de potencial vulnerabilidad que afecta de manera especialmente sensible al transporte de mercancías por carretera lo encontramos cuando esos vehículos están conectados a un Sistema de Gestión de Flotas que también puede ser vulnerado por un atacante "con la intención de obtener información de rutas, conductores, clientes, mercancías… o, incluso, modificar parámetros vitales de decenas de vehículos al mismo tiempo con la finalidad de llevar a la quiebra una empresa", advierte Azucena Hernández.

Nuevo reglamento europeo

Precisamente para atajar este problema de seguridad el 23 de junio de 2020 la Unión Europea aprobó el Reglamento UNECE/R155 que regula la ciberseguridad de los vehículos. El objetivo de esta normativa, "a grosso modo", es establecer las medidas uniformes necesarias para crear un sistema de gestión de ciberseguridad -CSMS- en los vehículos. Es decir, un sistema que trate el riesgo asociado con las amenazas y que proteja los vehículos de ciberataques.

> En la evaluación de ciberseguridad del vehículo se comprueba si el coche, camión, autobús, furgoneta o remolque cumple con los 70 requisitos de ciberseguridad que marca la Unión Europea en su Reglamento UNECE/R155.

Según aclaran desde Eurocybcar, la normativa diferencia claramente dos apartados: la evaluación técnica del nivel de ciberseguridad del vehículo -que quiera ser homologado- y el Sistema de Gestión de la Ciberseguridad del fabricante y del proceso de fabricación del vehículo.

En la evaluación de ciberseguridad del vehículo se comprueba si el coche, camión, autobús, furgoneta o remolque cumple con los 70 requisitos de ciberseguridad que marca la UNECE/R155. Estos 70 requisitos -definidos por las vulnerabilidades que se deben mitigar- se organizan en 7 apartados, según el tipo de amenaza:

- Relacionadas con los **servidores Back-End.** estos servidores son los hacen que todo el sistema informático de los vehículos o las redes informáticas internas del fabricante funcionen.
- Relacionadas con los **canales de comunicación** que usa el vehículo para conectarse con su entorno -por ejemplo, otros vehículos o la infraestructura-.
- Relacionadas con las **conexiones del vehículo** y su conectividad externa, ya que se deberán evitar que se puedan manipular funciones remotas, como la llave, el inmovilizador o las conexiones telemáticas del vehículo.
- Relacionadas con los **datos/código del vehículo.** En este apartado, se marcan requisitos para proteger la privacidad de las personas o para evitar la manipulación de datos del vehículo -kilometraje, velocidad de conducción, enviar mensajes falsos e indicaciones al conductor, etc.-.
- Relacionadas con los **pro-**

3 PREGUNTAS A: AZUCENA HERNÁNDEZ, CEO EUROCYBCAR

*"El futuro pasa por los **vehículos autónomos,** que basan sus decisiones en la información que obtienen de los sensores que incorporan, que **son vulnerables"***

¿Cree que hemos pasado por alto la seguridad en todo este proceso de avance de la conectividad que está experimentando el transporte por carretera en estos últimos años?

Lo más importante, de cara a la ciberseguridad, es que estos sistemas basan su funcionamiento en sensores, rádares o cámaras, y en EUROCYBCAR ya tenemos casos registrados de investigadores que han conseguido "engañar" a esos dispositivos para que el vehículo tome una mala decisión mientras circula y termine saliéndose de la carretera, como así demostró un investigador de la universidad de Corck que atacó con éxito los sensores de las ADAS de un vehículo… y no podemos olvidar que el futuro pasa por los vehículos autónomos, que basarán gran parte de las decisiones que tomen en la información obtenida por los sensores que incorporan, lo que requerirá un mayor nivel de ciberseguridad que evite que las decisiones adoptadas por el vehículo pongan en peligro la vida de los pasajeros.

¿Habéis realizado alguna auditoría para algún fabricante de vehículo industrial? ¿Qué sistemas, a vuestro juicio, son más susceptibles de poder ser "hackeados"?

En el caso de los vehículos industriales, en EUROCYBCAR hemos trabajado tanto en el vehículo en sí mismo, como en el Sistema de Gestión de Flotas, ya que las vulnerabilidades a las que se exponen se amplían en el caso de que esté interconectados a un gestor y al resto de vehículos de la flota.

Estableciendo esa diferencia, en lo que respecta al vehículo, los sistemas más vulnerables son todos aquellos que establecen comunicaciones inalámbricas tanto dentro del propio vehículo, como las que se establecen con el exterior -con otros vehículos, con infraestructuras, internet…-. Al ser comunicaciones que no requieren de un acceso previo al interior del vehículo, son las más explotadas por los crackers, que pueden llegar a encontrarse a cientos de kilómetros.

Desde vuestra experiencia, ¿puedes contarnos algún caso concreto que hayáis detectado, o que se haya hecho público?

Uno de los casos más destacados, que afectó al sistema de control flotas de miles de camiones en todo el mundo, fue el que sucedió en 2019, cuando un cracker -denominado L&M- accedió a más de 7.000 cuentas de usuarios de iTrack y a más de 20.000 cuentas de ProTrack, dos aplicaciones que utilizan las empresas de logística para monitorizar y gestionar las flotas de vehículos a través de los sistemas de seguimiento de GPS. El cracker fue capaz de conocer la geolocalización exacta de camiones en Sudáfrica, Marruecos, la India o Filipinas. Pero, lo más preocupante fue que, en algunos de los vehículos localizados, el software le permitía apagar sus motores de forma remota… aunque, por suerte, sólo si estaban parados o se desplazaban a una velocidad inferior a los 16 km/hora.

Un ejemplo de potencial vulnerabilidad que afecta de manera especialmente sensible al transporte de mercancías por carretera lo encontramos cuando esos vehículos están conectados a un Sistema de Gestión de Flotas que también puede ser vulnerado por un atacante.

cedimientos de actualización de los vehículos, entre las que se contemplan las amenazas que afecten a los procesos de actualización de los sistemas informáticos de los vehículos, ya sean inalámbricas -Over The Air / OTA- o mediante una descarga de internet.

• Relacionadas con **acciones humanas no intencionadas,** por lo que se deberán de evitar, entre otras amenazas, que alguien con acceso al vehículo pueda introducir un virus de forma involuntaria si lo engaña un ciberdelincuente.

• Relacionadas con otras posibles **amenazas que podrían explotarse** si no se protegen o refuerzan lo suficiente, por lo que se evitarán, entre otras amenazas, fallos de software o que se reemplacen elementos del vehículo que cumplan con la norma por otros que la incumplan.

Es importante reseñar que la normativa indica los 70 requisitos que debe cumplir un vehículo, pero no qué tipo de pruebas se deben realizar para saber si un vehículo puede obtener el certificado APTO de ciberseguridad. Es decir, a los fabricantes se les proporciona un listado con los riesgos que deben evitar en sus modelos a lo largo de todo el ciclo de vida del vehículo pero, por el momento, deben de ser ellos quienes piensen cómo solucionarlo, aunque el certificado deberá emitirlo una entidad externa.■

Según informa Eurocybcar, en 2021 se ha batido el récord de ciberataques a vehículos de todas las marcas y en todos los países. De manera remota, se han robado coches, acelerado y frenado vehículos en marcha o alterado los sistemas y tecnologías incluidos en todo tipo de automóviles.

NEW
NEW
NEW
NEW

WWW.EMPLEO.AUTONOMOSENRUTA.COM

¡¡MÁS DE 500 OFERTAS DE EMPLEO PUBLICADAS EN 2021!!

▶ **Más de 150 empresas han confiado en nosotros para encontrar conductores.**

▶ **Más del 80% de los conductores han encontrado o mejorado sus condiciones de trabajo.**

Entra en WWW.EMPLEO.AUTONOMOSENRUTA.COM
y publica tu oferta o demanda de empleo