LA NUEVA LEGISLACIÓN EUROPEA PRETENDE DEFENDER A TODOS LOS VEHÍCULOS FRENTE A LOS PIRATAS INFORMÁTICOS

¿Protegidos frente a los "ciberataques"?

Desde el pasado mes de julio los vehículos nuevos que llegan al mercado están más protegidos. A partir de ahora **deben contar con un certificado de ciberseguridad**, que protege también a las denominadas "cajas negras", que ya son obligatorias en todos los coches nuevos.

• S. L.

Los fabricantes han ido incorporando más tecnología inteligente en los nuevos vehículos. Todos estos elementos pueden facilitar el uso y seguridad de un automóvil, pero, como pasa en todos los entornos industriales, cuando se introducen nuevas tecnologías, también aumenta el riesgo de ciberataques. También está expuesta la conocida como "caja negra", obligatoria en todos los coches nuevos desde el pasado 7 de julio, ya que puede sufrir el riesgo de manipulación por parte de terceros.

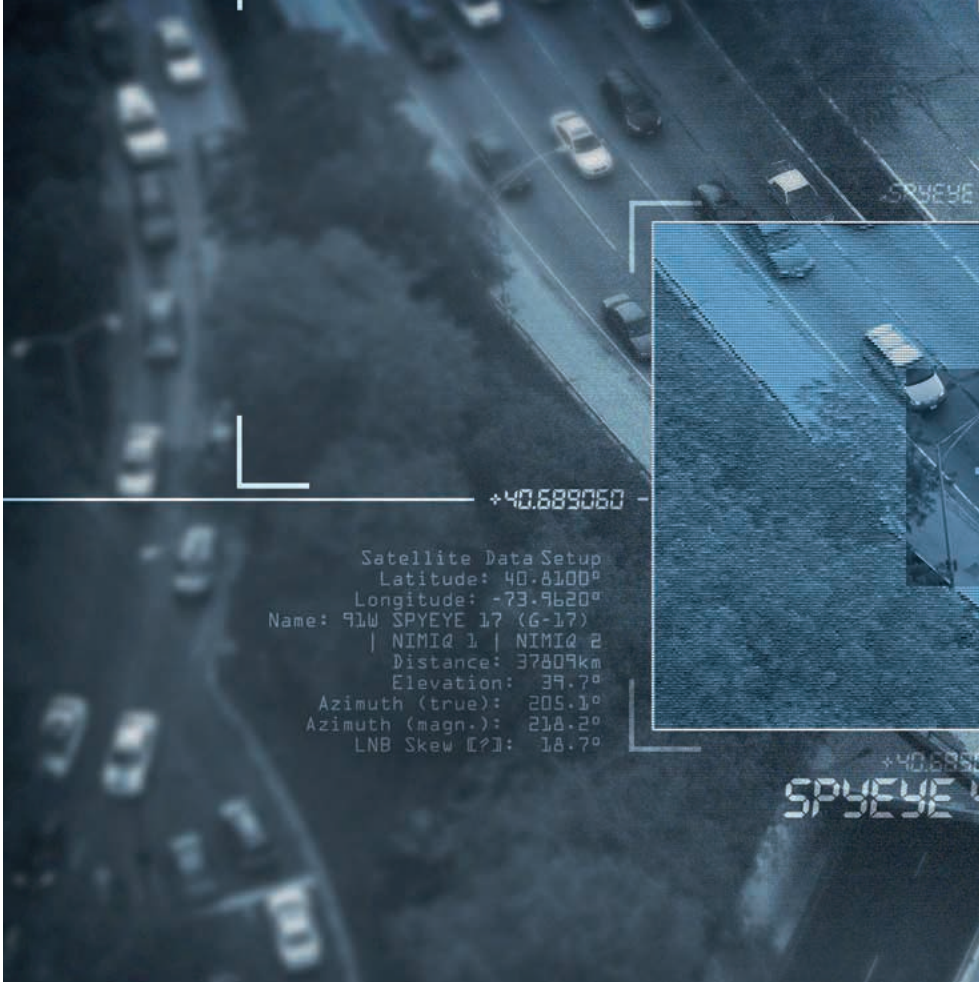
Por todo ello, la Unión Europea tomó cartas en el asunto al establecer regulaciones estandarizadas para todos los automóviles vendidos en Europa, y que se ha materializado en los reglamentos europeos UN R155 y UN R156, reglas que acaban de entrar en vigor este pasado mes de julio. Estas regulaciones establecen un sistema de homologación de ciberseguridad que todos los vehículos -coches, camiones, furgonetas, autobuses y autocaravanas- que se fabriquen o se vendan en Europa deberán superar antes de poder ser comercializados dentro de la Unión Europea. En caso de incumplimiento, los fabricantes podrían enfrentarse a sanciones de hasta 30.000 euros por vehículo.

El fabricante puede obtener esta homologación de cualquier Autoridad de Homologación europea, responsable de la aplicación y cumplimiento de dicha normativa.

Ciberprotección

Entre las compañías especializadas en ciberseguridad, la empresa Eurocybcar, ubicada en Vitoria-Gasteiz, mide y certifica el nivel de ciberseguridad de los vehículos. Al someterlos a la batería de pruebas de los test que ellos realizan se comprueba si el fabricante ha implementado mitigaciones que eliminen o minimicen los riesgos y vulnerabilidades que señala ▶▶

¿Protegidos frente a los "ciberataques"?



la normativa europea de ciberseguridad para vehículos, verificando si esos modelos protegen la privacidad -los datos- y, sobre todo, la vida del conductor y los pasajeros de forma adecuada.

Es importante comprobar si los principales sistemas de seguridad del vehículo están debidamente ciberprotegidos, como el E-Call, los frenos, los airbags, los asistentes de conducción, etc., con el fin de evitar ser vulnerables en caso de que sean atacados por un ciberdelincuente y que este pueda robar datos e información personal, modificar parámetros del vehículo para frenarlo, acelerarlo o bloquearlo o, incluso, tomar el control del coche de forma remota, poniendo en peligro la integridad del propio vehículo, sus sistemas y, lo más importante, sus pasajeros.

EDR o caja negra

Como se ha señalado anteriormente, desde el pasado 7 de julio, todos los coches de nueva matriculación en España deben contar con una "caja negra". Así lo ha dictaminado la Unión Europea con el objetivo de mejorar la seguridad vial y reducir el número de accidentes en las carreteras. Estas "cajas negras" deben cumplir también los requisitos de ciberseguridad establecidos en la UNECE/R155, protegiendo de la manipulación de un tercero los datos y parámetros que se hayan almacenado tras un incidente.

"NO SE PUEDE ASEGURAR LA CIBERSEGURIDAD AL 100%"

AZUCENA HERNÁNDEZ, EUROCYBCAR

La caja negra es un sistema avanzado de ayuda a la conducción, o ADAS por sus siglas en inglés, que registra el momento previo y posterior de un accidente para poder saber qué ha ocurrido. De acuerdo a un estudio elaborado por el Parlamento Europeo, gracias a los ADAS podrían evitarse 25.000 muertes y más de 140.000 heridos graves en los próximos 15 años, e incluso conseguir alcanzar las cero muertes en carreteras europeas para 2050.

Estas cajas negras de los vehículos, conocidas técnicamente como EDR (Event Data Recorder), actúan como mecanismo de seguridad cuya funcionalidad es similar a la caja negra de los aviones: registrar datos, información, eventos y parámetros de conducción del momento en el que el vehículo se ve envuelto en un incidente durante la conducción, así como en los momentos anteriores y posteriores a que se produzca dicho incidente. Debemos tener en cuenta que un incidente puede implicar desde una frenada de emergencia ante un obstáculo, un derrape o una maniobra brusca hasta, en el peor de los casos, un accidente.

"Para ello, la EDR captura parámetros del vehículo de forma constante -nos explica Azucena Hernández, CEO de Eurocybcar-. *Esos datos se almacenan en una "memoria volátil" y son eliminados en un intervalo de tiempo predefinido por el fabricante con el objetivo de que, solamente, cuando algunos sensores -por ejemplo, los acelerómetros- o sistemas de seguridad se activan, los parámetros registrados se almacenen y no se borren de la memoria".*

La EDR tiene como objetivo recopilar información, tanto del vehículo como de sus ocupantes -pero no datos de imágenes ni de audios-. En caso de incidente, registra y almacena datos específicos, normalmente entre cinco segundos previos y los cinco segundos posteriores. De esta manera, se puede obtener valiosa información para ayudar a esclarecer las causas del incidente y evaluar el funcionamiento de los diferentes sistemas de seguridad activa y pasiva del vehículo.

El objetivo principal de los datos registrados en la EDR es poder ayudar a esclarecer los hechos ocurridos, facilitando enormemente los trabajos de investigación. Esta información también sirve para mejorar la seguridad de las carreteras y de los sistemas de los vehículos. Es decir, analizando estas informaciones es posible saber cómo ha ocurrido el accidente, las velocidades a las que ha ocurrido e incluso establecer hipótesis sobre la responsabilidad.

¿Son 'crackeables'?

"Por eso, es tan importante que se aplique correctamente la UNECE/R155 y se protejan los datos que almacenan las EDR. Por ejemplo, se ha dictaminado que el acceso al contenido de dichos datos se deberá hacer siempre a través de una conexión física, evitando la inalámbrica, ya que un acceso malintencionado podría modificar o eliminar estos datos, dificultando la investigación de los hechos", nos acla-

ran desde Eurocybcar. Nos preguntamos si estas "cajas negras" podrían ser fácilmente vulnerables y 'crackeables'. La CEO de Eurocybcar puntualiza que *"la ciberseguridad no se puede asegurar al 100%*". La tecnología está en constante evolución y si esta dispone de una conectividad exterior -incluso si no es inalámbrica- presenta vulnerabilidades que pueden ser explotadas por un ciberdelincuente que disponga de los recursos, la pericia y los conocimientos necesarios para acceder y manipular los datos que almacenan las EDR. *"Aunque, a fecha de hoy* -añade-, *no se tiene constancia de que se haya producido algún "crackeo" a una EDR (lo que no significa que se haya podido producir alguno), algo que puede obedecer a que es una tecnología que todavía no está implementada en un gran número de vehículos. Por otro lado, la ciberseguridad de un sistema se ve afectada por las vulnerabilidades del conjunto de elementos con los que interactúa. En el caso de las EDR, si bien el acceso a los datos almacenados puede estar "blindado", debemos tener en cuenta que esos datos se obtienen de elementos y sistemas externos que se podrían ver afectados por un ciberataque y, por tanto, la información "fake" sería aceptada como real por la EDR".* ◆

ENTREVISTA
AZUCENA HERNÁNDEZ
CEO de Eurocybcar

"Por seguridad, debemos comportarnos con los datos del coche como hacemos con el móvil"

¿Cuáles son los ciberataques más habituales que se están produciendo contra los vehículos?

Según nuestras investigaciones, los ataques más habituales realizados directamente contra los vehículos son los dirigidos a los sistemas de apertura. En concreto sobre el sistema Keyless Passive, que es la tecnología que permite abrir y/o arrancar el coche sin necesidad de utilizar la llave.

Su funcionamiento se basa en comunicaciones de radiofrecuencias en diferentes intervalos para tener varias líneas de comunicación, una para verificar y otra para abrir. Atacando este sistema los ciberdelincuentes pueden conseguir acceso al vehículo y arrancarlo para robarlo, sin activar ninguna alarma, y por lo tanto sin hacer ningún ruido.

Por otro lado, también están en auge los ataques contra los servidores de las marcas fabricantes con el objetivo de "robar" los datos privados de los clientes y proveedores y explotarlos o comercializar con ellos en la "Deep Web".

¿Cómo se evita que personas ajenas puedan espiar y apropiarse de nuestros datos?

Lo primero y lo más importante es que cuando alguien vaya a utilizar, comprar, alquilar o compartir un vehículo exija que ese vehículo sea ciberseguro... o, por lo menos, que le garanticen que sus datos y su vida -y los de las personas que le acompañan- no corren ningún tipo de peligro cuando viaja a bordo.

A nivel práctico, un buen consejo es que el usuario se comporte con su vehículo de la misma forma que se comportaría con un ordenador o su móvil: cambiar de forma periódica las contraseñas de las diferentes tecnologías que incorpora el vehículo, como son el Bluetooth o la Wifi, y mantener actualizado el software del vehículo, ya sea acudiendo al taller oficial de la marca o autorizando las actualizaciones remotas que solicita el fabricante.

También hay que tener en cuenta que al dar de baja el vehículo es importante eliminar todos los datos que tiene almacenados... A nadie se le ocurriría vender su móvil sin haberlo "vaciado"... ¿verdad?

Por último, si decide instalarse en el móvil la app que ofrecen la mayoría de fabricantes, debe crear un usuario y una contraseña muy robusta y cambiarla periódicamente, para evitar que si alguien accede al móvil pueda conocer la ubicación del vehículo, los recorridos que efectúa, abrir los seguros de las puertas... y esto, que suena a ciencia ficción ya ha sucedido. En Australia, en el año 2021, a través de la aplicación que ofrece un fabricante y que el usuario se descarga en el móvil para conocer en todo momento dónde está el vehículo, abrir y cerrar las puertas... un hombre acosó y espió a su exnovia, llegando incluso a arrancar y parar el motor de forma remota. Hablamos de los "nuevos ciberdelitos".

Con esta nueva normativa comunitaria, ¿podemos estar ya seguros en el coche en materia de ciberataques?

Aunque los fabricantes están dedicando un gran esfuerzo a mejorar el nivel de ciberseguridad de los vehículos, es tarea de todos contribuir también con nuestro esfuerzo y concienciarnos para conseguir que se alcance un alto nivel de ciberseguridad que proteja correctamente tanto los datos -la privacidad- como la integridad y la vida de las personas que viajan a bordo de un vehículo.

Por eso, quienes nos dedicamos a trabajar por conseguir que en Europa y en el mundo la movilidad sea más cibersegura, seguiremos luchando para minimizar y eliminar las ciberamenazas que puedan existir en cualquier elemento que forma parte del ecosistema de la movilidad: coches, camiones, autobuses e infraestructuras de movilidad.