MOTOR

NORMATIVA EUROPEA

Si los 'hackers' roban a la DGT, que no lo hagan con los coches

● Desde el día 6, deberán llevar un certificado de ciberseguridad para venderse ● Tráfico investiga el robo de millones de datos

FÉLIX CEREZO MADRID

La noticia saltó ayer al mediodia: la Guardia Civil de Tráfico está investigando el posible robo de los datos de conductores –cerca de 28 millones en España– y de sus vehículos –unos 32 millones– que habrían sido sustraídos de las bases de datos de la DGT y puestos a la venta en Internet.

«Tenemos que ver si es así, porque, a veces, son anuncios falsos para lograr repecursión» señalaron fuentes de Tráfico a EL MUNDO, después de que *El Confidencial* publicase que esa información se ofrecía, desde el pasado 13 de mayo, en un foro dedicado a la compraventa de información robada en ataques informáticos. Los delincuentes habrían obtenido desde las matrículas de los vehículos al nombre completo de los dueños, su DNI y domicilio o los datos del seguro.

«Hace dos semanas, detectamos a varios usuarios sospechosos que habían intentado entrar en la base de datos para recabar información. Se les cortó el acceso, fueron identificados y están siendo investigados» añadieron desde Tráfico a este diario. Las mismas fuentes recordaron, además, que este tipo de cibertataques son frecuentes en los distintos organismos y empresas. Sin ir más lejos, a Ticketmaster –la empresa de venta de entradas on line – le han robado los datos de más de 500 millones de clientes en plena gira de Taylor Swift.

Bueno, pues no piense que eso solo les pasa a grandes corporaciones o instituciones a las que simplemente dañar o hacer negocio con ellas. Su coche también es susceptible de sufrir un ataque informático.

Piense, por ejemplo, que al llegar esta mañana a cogerlo, no ha tenido que usar la llave para abrirlo. El sistema *keyless* ha reconocido que la llevaba en el bolsillo y le ha franqueado el paso. Lo siguiente que ha hecho el automóvil es enlazarse con su smartphone y lanzar en el navegador la ruta que ya había seleccionado en casa. Bueno, también mientras se tomaba el café, usó la app de la marca para ordenarle que el habitáculo estuviese a la temperatura ideal cuando llegase. Por último, subido al interior y antes de arrancar, el coche le avisó de una actualización de software pendiente de descargarse, por si quería hacerlo en ese momento. Y lo hizo.

DISTINTOS TIPOS DE ATAQUES

'KEYLESS'. O acceso sin llave. El atacante lo que hace es replicar la información que envía el mando a la centralita para así poder abrir el coche y llevárselo que hay dentro o incluso el vehículo.

DENEGACIÓN DE SERVICIO. Aquí se trata de bloquear todas las comunicaciones de los automóviles conectados y, por lo tanto, representa un alto riesgo para la seguridad de las personas.

RECARGA ELÉCTRICA. Relativamente nuevo, el 'hacker' aprovecha para infectar el vehículo si está conectado a un poste de recarga, con el que intercambia información.

'E-CALL'. Si lo manipulan, en caso de un accidente puede que la asistencia médica se retrase o que no venga. También es factible engañar al GPS o forzarle a dar indicaciones erróneas y peligrosas.

MANEJO. Es una de las situaciones más delicadas. De forma remota, se toma el control de la dirección y los frenos: se altera o apaga el motor o la batería de un eléctrico; se anulan sistemas de seguridad, etc.

Son solo algunas de las muchas ventajas que supone contar con automóviles cada vez más inteligentes y conectados: con usted, con la nube, con el propio fabricante y con las infraestructuras.

La otra cara de la moneda es que, con esas operaciones, ha abierto hasta cuatro veces la puerta para que su coche sufra un ciberataque. ¿Peligroso? Pues depende. Como en el caso de la DGT, puede tratarse solo de obtener un beneficio económico o usarlos de forma fraudulenta. Pero es famosa la iniciativa de dos informáticos que, ya en 2015, demostraron ser capaces de abrir y tomar de forma remota el control de un Jeep mientras un periodista –al que usaron como cobaya– iba al volante. Un año antes, el FBI estadounidense había advertido de los potenciales peligros de los automóviles autónomos si caían en las manos equivocadas.

ACTIVACIÓN REMOTA

Y eso que hablamos de la prehistoria en cuanto a la conectividad y funcionalidades de un automóvil moderno. Hoy, podemos comprar un Tesla que es casi autónomo, pero con parte de esos sistemas latentes porque no hemos pagado por ellos o no están autorizados en todos los países. Si un día queremos o ya podemos usarlos, al fabricante le basta con activarlos de forma remota.

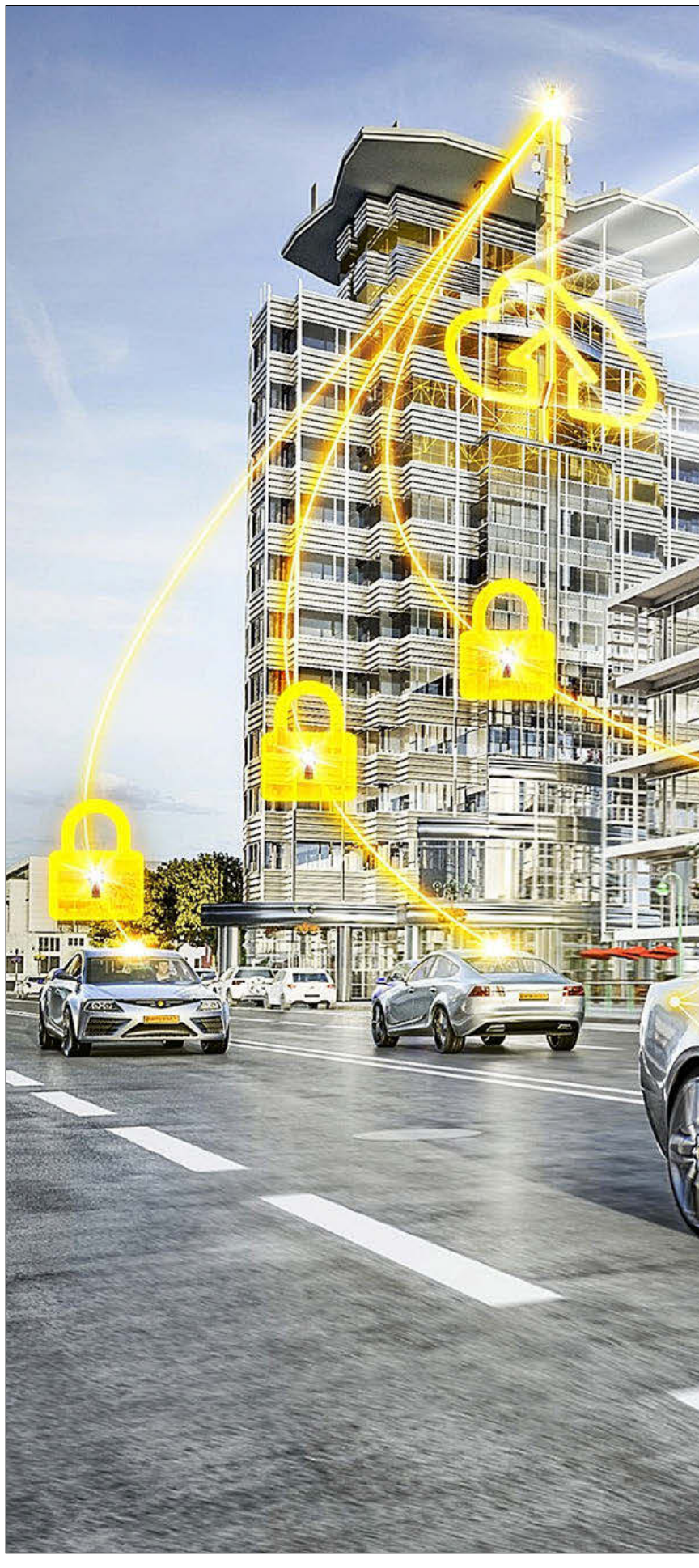
Desde el próximo 6 de julio, que alguien que no sea Tesla dé esa orden (o la contraria para un asistente activo) será mucho más complicado. Desde esa fecha no se podrán vender automóviles nuevos que no cumplan con las normas R155 y 156, promovidas por la ONU y a las que también se han sumado Japón y Corea del Sur, no así EEUU. «Ambas suponen un punto de inflexión en materia de ciberseguridad en el sector» señala Alejandro Prieto Castro, del Instituto Nacional de Ciberseguridad (Incibe).

La segunda de ellas busca garantizar que las actualizaciones de software se realicen de forma segura, sin introducir vulnerabilidades adicionales. La primera forma parte del mismo paquete legislativo que ha hecho obligatorios desde julio hasta ocho nuevos asistentes de seguridad ADAS. Y como pasaba con éstos, desde hace dos años ya era obligatoria para los vehículos de nueva homologación y que en este caso son todos, desde un coche a un camión.

Su alcance es mucho mayor, pues se centra en la protección de los automóviles contra ciberataques y la gestión eficiente de incidentes, abarcando desde el proceso de diseño y los componentes hasta el final de su vida útil. La norma exige hacer frente a 70 amenazas de todo tipo, a lo que hay que añadir dos hechos. Por un lado, las hasta 150 centralitas y 100 millones de líneas de códigos –cuatro veces más que un caza de combate– que tiene un automóvil moderno; por otro, que el peligro puede estar oculto en algo tan sencillo como la música que descargamos a través de un pendrive.

Además, ni la UNECE ni la UE han diseñado en este tiempo (el proyecto arrancó en 2020) un protocolo común de las pruebas a superar para lograr el apto. Ni quién las debe llevar a cabo. Sólo que esa validación la tendrá que realizar un organismo independiente, no el fabricante por su cuenta. En España, el Ministerio de Industria o laboratorios asociados como el Insia, el Inta o Idiada. Son los mismos que realizan las homologaciones técnicas y de consumos.

De hecho, este periódico contactó con varios fabricantes que remiten a



Simulación del flujo de información y datos que genera un automóvil. EM

LOS AUTOMÓVILES MODERNOS ESTÁN CONECTADOS A NUESTRO MÓVIL, A LA NUBE, A LAS CARRETERAS...

un tema «complejo» y sensible en el que van de la mano de Industria; que sus coches cumplen con la norma y, como mucho, adelantan que supondrá un aumento de precio de «entre 100 y 200 euros».

En cambio, si mintiesen y las homologaciones de los vehículos fueran fraudulentas, se arriesgan a una sanción de hasta 30.000 euros por cada automóvil. Una multa que se estableció para evitar que se repitieran engaños como el del *dieselgate*.

En este contexto cobra especial relevancia el papel de la empresa Eurocybcar, radicada en Vitoria y que está respaldada por Aenor (ver información adjunta).

METODOLOGÍA ÚNICA

Según su CEO, Azucena Hernández, han sido los primeros en desarrollar y patentar una metodología (y herramientas informáticas) que «certifican la ciberseguridad de los vehículos» al evaluar qué aspectos de los exigidos se cumplen, cuáles no y cómo resolver los problemas que se presenten. «Son pruebas que se realizan de forma estandarizada y que se pueden aplicar a los distintos modelos de automóviles» señala a este periódico.

Son pruebas de tres tipos. De acceso físico, comprobando si se pueden manipular elementos como el ABS, los frenos o la dirección. Las segundas verifican los accesos remotos, analizando sistemas inalámbricos como la apertura sin llave, el wifi, el Bluetooth o la llamada de emergencia E-call. Finalmente, se ensayan las distintas aplicaciones que los fabricantes integran en sus coches.

Aunque la cosa no se detiene ahí, como señala Hernández, ya que las exigencias de ciberseguridad se irán extendiendo al resto de la cadena de valor, incluyendo concesionarios y talleres. Precisamente en abril entró en vigor el llamado procedimiento SERMI, solo exigible en la UE y que garantiza que los talleres (oficiales y multimarca) puedan realizar el mantenimiento y reparación de los vehículos sin comprometer su integridad.

Por su parte, la directiva 2022/2555 también de la Unión Europea señala a la industria de automoción como una de las «críticas» de cara a protegerla frente a ciberataques. Una categorización que también se hará extensible al sector del transporte por carretera.

AZUCENA HERNÁNDEZ

CEO DE EUROCYBCAR

«Podemos ser el equivalente de lo que hace EuroNCAP»

F. C. EL MUNDO

En enero de 2022, la moto eléctrica NUUK Cargopro se convirtió en la primera en lograr el certificado de ciberseguridad según la normativa UNECE R155 y la metodología de la compañía española Eurocybcar. Su CEO, Azucena Hernández, señala que ese paso fue decisivo para que la ONU haya decidido incluir a estos vehículos en una disposición de las que los había excluido de inicio.

Con una plantilla que llega ya a los 40 empleados, la compañía radicada en Vitoria trabaja también con cuerpos policiales como la Guardia Civil y la Ertzaintza. «Por ejemplo, para que verifiquemos si sus vehículos, entre los que están los de altos cargos, han sido sometidos a algún tipo de ataque». Uno de esos riesgos sería grabar las conversaciones que se mantienen en el interior del vehículo. En el caso de la policía autonómica vasca, acaban de ganar un contrato por un importe de 6,3 millones de euros para la «evaluación e implementación de medidas de ciberseguridad en los vehículos de la Ertzaintza», que será pionera en España en este aspecto.


EL MUNDO

Según la directiva, su compañía tiene «un potencial de negocio brutal» y dice gracias a su metodología podrían asimilarse al funcionamiento de EuroNCAP.

Este organismo paneuropeo sin ánimo de lucro lleva desde el año 1997 midiendo la seguridad de los vehículos a través de distintos ensayos de choque. De ahí resulta una valoración –el máximo son cinco estrellas– según lo que proteja a ocupantes, ciclistas y peatones.