Estudio sobre el transporte por carretera: la digitalización avanzan rápidamente pero la conciencia sobre ciberseguridad todavía está en sus inicios

* Existe una importante brecha de ciberseguridad entre las grandes y pequeñas empresas
* Hay un alto nivel de seguridad pero las bajas inversiones que pueden implicar riesgos
* Una nueva regulación es un paso importante hacia una mayor seguridad de los vehículos
* Es necesario una ampliación de las soluciones más adecuadas para la industria

8 de septiembre de 2020. La digitalización de la industria del transporte por carretera impulsada por la necesidad de ser más eficiente avanza rápidamente en todas las esferas comerciales, pero la conciencia general de necesidad de protección contra los ciberataques sigue siendo incipiente.

Este es uno de los principales resultados del estudio realizado por Continental "Commercial Vehicles 2020: Cybersecurity and Digitalization”. Es cierto que las soluciones de conectividad desempeñan un papel cada vez más importante en la cadena de suministro y en el sector del transporte, ya que aumentan la eficiencia y ayudan a reducir los costes en un mercado cada vez más competitivo. "Sin embargo la conectividad también aumenta los riesgos de ciberataques en las compañías de transporte. Al mismo tiempo, y en concreto las empresas más pequeñas, siguen dudando en invertir en protección para sí mismas y sus flotas de estos ataques", explica el Dr. Mathias Dehm, director de Investigación y Procesos para la Seguridad de Productos de Continental.

Unas soluciones y presupuestos adaptados a sus necesidades, así como la reciente regulación en el campo de la ciberseguridad en los vehículos, puede mejorar considerablemente su postura en materia de ciberseguridad. Para el estudio, realizado por el Instituto Applied Social Science (INFAS), se entrevistó a expertos alemanes de diferentes asociaciones y autoridades además de a empresas de transporte por carretera y proveedores de servicios tecnológicos. Estas entrevistas fueron complementadas por un panel de expertos, para el que se realizaron entrevistas online a empresas alemanas de transporte por carretera y expertos en logística.

Alto grado de seguridad que puede entrañar riesgos

Otro de los resultados del estudio es que muchas compañías de transporte se sienten relativamente seguras ante un ciberataque; así, cerca de dos tercios de los entrevistados en el panel de discusión se consideraban estar protegidos contra ese tipo de ataques. Sólo la mitad de las empresas dispone de mecanismos de seguridad para protegerse de estos ciberataques, a sus flotas o sistemas de gestión de flotas. Tres cuartas partes no planean realizar más inversiones en los próximos 6/12 meses, pero esta sensación de relativa seguridad puede traer problemas.

“Aunque todavía las flotas no tienen en el centro de sus discusiones la ciberseguridad, éstas son objeto de este tipo de acciones por su tipo de carga, como por ejemplo mercancías peligrosas, su tamaño y la importancia económica. En consecuencia, existe un potencial peligro para estas empresas, como cuando los hackers cierran flotas para extorsionar y pedir dinero a cambio de un rescate,” comenta Mathias Dehm.

La ciberseguridad para una protección de la digitalización

“El estudio muestra que la ciberseguridad es algo crucial, especialmente en el sector del transporte por carretera, ya que sin conectividad es prácticamente imposible trabajar eficientemente. La ciberseguridad protege los beneficios que se obtienen de la digitalización, lo que es vital para los vehículos industriales, por lo que merece una mayor atención,” afirma Gilles Mabire, director de la Unidad de Negocio en Continental de Commercial Vehicles and Services (CVS). “En el futuro, el propio valor de la ciberseguridad será más evidente, como por ejemplo cuando el aumento de la digitalización cause más ataques en los sistemas de las empresas de transporte y logística. Esto también puede aumentar el interés por invertir en este aspecto”.

**Ciberseguridad al alcance de las pequeñas flotas**

Existe una regla general: cuanto más grande sea la empresa, más importancia se da a la ciberseguridad. “Existe una gran brecha entre las grandes compañías y las pequeñas. Las grandes compañías pueden desarrollar estrategias, contratar especialistas en sistemas IT y de ciberseguridad de automoción, así como establecer sus propias unidades cibernéticas, pero las más pequeñas a menudo carecen de la conciencia y los medios financieros para hacerlo", dice Dehm.

Esto es un problema, teniendo en cuenta los bajos márgenes en los que se mueve el sector de la logística, donde cada céntimo invertido cuenta. Según una encuesta realizada por German Federal Office for Goods Transport, en la industria hay una mayor presencia de pequeñas y medianas empresas.[[1]](#footnote-2) Además a de la regulaciones legales, las empresas (especialmente las pequeñas) deberán tener acceso a soluciones asequibles que se adapten a sus necesidades. “No hay ninguna duda en que la ciberseguridad debe ser accesible para todos,” comenta Ido Ben Ami, Vice President Research & Development, Argus Cyber Security. “Por esta razón, se han puesto a disposición soluciones escalables de ciberseguridad, para permitir que las pequeñas empresas amplíen sus capacidades a medida que crezcan. Por ejemplo, se puede adaptar a las necesidades y recursos específicos de cada organización un centro de operaciones de seguridad que permita a los gestores de flota vigilar, detectar y responder a estos ataques.

La ciberseguridad requiere de una visión holística de la empresa

Cuando se trata de inversiones en ciberseguridad, a muchas empresas les resulta difícil utilizar de manera sostenible soluciones de seguridad, ya que se considera terminado el proceso cuando el software se programa. Sin embargo, se requiere una inversión continua para mantener los sistemas actualizados, lo que puede implicar una customización adecuada al sistema de la empresa, realización de actualizaciones periódicas, formación del personal y, por último, apoyo. En resumen, una inversión particular no es suficiente para abordar el problema de la ciberseguridad de manera integral y afianzarlo permanentemente en la empresa. "Además de los propios camiones, la ciberseguridad también afecta a toda la infraestructura informática, incluidos los sistemas de gestión de flotas o la organización del trabajo. De ser posible, estas áreas de responsabilidad deberían agruparse “en un todo” para que todas los interfaces entre las áreas sean cubiertas", señala Mathias Dehm de Continental.

Uniformidad en las normas: un paso importante hacia la seguridad en los vehículos

Se han dedicado más de tres años para establecer una nueva regulación que establezca unas normas uniformes en materia de ciberseguridad en los vehículos. El reglamento elaborado por el grupo de trabajo WP.29 de la Comisión Económica de las Naciones Unidas para Europa (UN ECE) examina los requisito de seguridad durante el proceso de homologación del vehículo. Además de revisar las medidas de seguridad adecuadas, también audita los procesos de las empresas, entre otras cosas. Esto garantiza que la ciberseguridad se aborde durante el Desarrollo e industrialización de los componentes y software. El documento UN ECE WP .29 será introducido por fases a mediados del 2022 y se aplicará a todos los tipos de vehículos nuevos matriculados a partir de Julio 2024, lo que supone un paso importante hacia una mayor seguridad. "Dado que el nivel de conectividad es cada vez mayor en áreas como la conducción autónoma y las aplicaciones relacionadas con 5G, la ciberseguridad seguirá ganando importancia y deberá ser considerada en nuevas áreas de aplicación", afirma Gilles Mabire.

Información sobre el estudio

Para realizar el estudio sobre "Digitalización y ciberseguridad en los vehículos industriales" encargado por Continental, INFAS (Instituto de Ciencias Sociales Aplicadas) interrogó a expertos de asociaciones, autoridades, empresas de transporte y proveedores de servicios tecnológicos acerca de la ciberseguridad y los desafíos para la industria del transporte y la logística causados por la digitalización. De diciembre de 2019 hasta febrero de 2020 se realizó un total de diez entrevistas cualitativas tanto telefónicas o presenciales. La encuesta incluía preguntas sobre temas como la digitalización en la empresa, la importancia de la ciberseguridad, amenazas, medidas, estructuras, necesidades y el deseo de mejorar. La encuesta fue complementada por un panel de expertos, para el que el INFAS realizó encuestas online en empresas del sector del transporte, de logística y de transporte. Con este fin, entre febrero y mayo se contactó con empresas de transporte, logística y transporte por carretera de Alemania, mediante selección estadística aleatoria. Los resultados evaluados de los 45 participantes proporcionan una visión del estado de la digitalización de la industria, el uso de soluciones de software y el tema de la ciberseguridad en la industria de vehículos industriales.

Continental desarrolla tecnologías inteligentes y servicios pioneros para la movilidad sostenible y conectada para el transporte de personas y mercancías. Fundada en 1871, la empresa de tecnología ofrece soluciones seguras, eficientes, inteligentes y asequibles para vehículos, máquinas, tráfico y transporte. En 2019, Continental generó ventas de 44.500 millones de euros y actualmente cuenta con alrededor de 230.000 personas en 59 países.

Continental desarrolla tecnologías pioneras para hacer el transporte comercial más seguro, eficiente y conectado. Los productos y servicios de la empresa tienen un impacto medible para los fabricantes de vehículos industriales y la posventa que se benefician de una amplia cartera de productos y sistemas plenamente integrados. Estos productos van desde neumáticos, monitorización digital de neumáticos, gestión de flotas, soluciones telemáticas, dispositivos electrónicos de registro (ELD) y tacógrafos, mangueras, muelles de aire, unidades de control electrónico (ECU), pantallas, sistemas de transmisión y escape de gases, sensores, sistemas avanzados de asistencia a la conducción, así como eHorizon y servicios basados en la nube. En 2019, la participación de Continental en las ventas globales para vehículos industriales, sistemas y servicios fue de 5.000 millones de euros.

Contacto Prensa

Silvia Cano

Responsable de Comunicación

Comunicación / Interior

Continental Automotive Spain S.A

Phone: +34 637 089 688

silvia.cano@continental-corporation.com

**Press portal:** www.continental-press.com

**Media center:** www.continental.com/media-center

Imágenes y pie de foto

|  |  |
| --- | --- |
| Continental\_PP\_Study\_Cybersecurity\_Infographics\_1 | La industria se siente relativamente segura en términos de ciberseguridad y por ello sólo realiza inversiones modestas; algo que conlleva riesgos |
| Continental\_PP\_Study\_Cybersecurity\_Infographics\_2 | La mayoría de las compañías de flotas dependen de los fabricantes y de las visitas a talleres cuando se trata de mantener el software actualizado. Sólo unos pocos tienen una visión general completa de si el software del vehículo está actualizado. |
| Continental\_PP\_CV\_Cybersecurity\_wAttacks | El reglamento de la Naciones Unidas WP.29 establece por primera vez normas uniformes de ciberseguridad para los vehículos. Además, las soluciones a medida más cercanas a las pequeñas empresas típicas de la industria pueden proporcionar más seguridad de los vehículos. |
|  |  |

1. <https://www.bag.bund.de/DE/Navigation/Verkehrsaufgaben/Statistik/Ustat/ustat_node.html> [↑](#footnote-ref-2)