Studie zum Straßengüterverkehr: Digitalisierung schreitet voran, Bewusstsein für Cybersecurity noch am Anfang

* Cybersecurity-Kluft zwischen den großen Playern und kleineren Unternehmen
* Relativ hohes Sicherheitsgefühl und niedrige Investitionen können Risiken bergen
* Neue Cybersecurity-Regulierung wichtiger Schritt für mehr Fahrzeugsicherheit
* Für die Branche adäquate Lösungsangebote müssen weiter ausgebaut werden

Schwalbach, September 2020. Während die Digitalisierung im effizienzgetriebenen Straßengüterverkehr in allen Unternehmensbereichen schnell voranschreitet, steht das Bewusstsein für den Schutz vor Cyberangriffen noch am Anfang. Das ist eines der Ergebnisse der „Nutzfahrzeugstudie 2020 – Cybersicherheit und Digitalisierung“ des Technologieunternehmens Continental. Zwar nehmen vernetzte Lösungen in Lieferkette und Transport eine immer wichtigere Rolle ein, weil sie im starken Wettbewerb in der Transportbranche Effizienz-Vorteile bringen und Kosten senken. „Mit der Vernetzung steigen aber auch die Risiken für Cyberangriffe. Gleichzeitig sind insbesondere kleinere Unternehmen beim Schutz von Fuhrpark und Unternehmen vor Angriffen noch recht zögerlich, was Investitionen angeht“, erläutert Dr. Mathias Dehm, der den Bereich Forschung und Prozesse für Produktsicherheit bei Continental leitet. Auf ihre Bedürfnisse und Budgets stärker zugeschnittene Lösungen und eine kürzlich verabschiedete Regulierung des Feldes Fahrzeug-Cybersicherheit können Abhilfe schaffen. Für die Studie hat das infas Institut für angewandte Sozialwissenschaft Experten in Verbänden, Behörden, Speditionen und Technologiedienstleister im Rahmen von qualitativen Leitfadeninterviews befragt. Ergänzt wurde die Befragung durch ein Branchenpanel, für das infas Unternehmen der Transportbranche, Logistiker und Spediteure online interviewt hat.

Hohes Sicherheitsgefühl kann Risiken bergen

Ein weiteres Ergebnis der Studie: Viele Unternehmen fühlen sich relativ sicher vor Cyberangriffen. Rund zwei Drittel der Befragten des Branchenpanels sehen sich sehr gut vor einem solchen Angriff geschützt, und nur rund die Hälfte der Unternehmen hat Abwehrmaßnahmen für ein Angriffsszenario auf Logistik- oder Flottenmanagementsysteme getroffen. Drei Viertel planen keine größeren Investitionen in den kommenden sechs bis zwölf Monaten. Dieses relativ hohe Sicherheitsgefühl kann auch Risiken bergen. „Flotten standen zwar bislang nicht im Rampenlicht der Diskussion um Cyberkriminalität, sind aber aufgrund ihrer Ladung wie zum Beispiel Gefahrgut, ihrer Flottengröße und ihrer wirtschaftlichen Wichtigkeit lohnende Angriffsziele. Es gibt also durchaus Gefährdungspotenziale für Logistikunternehmen, beispielsweise wenn kriminelle Hacker Flotten stilllegen, um Lösegeld zu erpressen“, sagt Mathias Dehm.

Cybersicherheit schützt die Gewinne der Digitalisierung

„Die Studie zeigt: Gerade für den effizienzgetriebenen Straßengüterverkehr ist Cybersicherheit von großer Bedeutung, denn ohne Konnektivität ist effizientes Arbeiten kaum möglich. Cybersicherheit schützt also die Gewinne der Digitalisierung, die gerade für die Nutzfahrzeugbranche lebenswichtig ist. Daher verdient sie mehr Aufmerksamkeit“, sagt Gilles Mabire, der die Geschäftseinheit Commercial Vehicles und Services (CVS) bei Continental leitet. „Es kann gut sein, dass der Wert des Gutes Cybersecurity zukünftig steigt, etwa wenn durch die zunehmende Digitalisierung auch die Zahl der Angriffe auf die Systeme von Transport- und Logistikunternehmen zunimmt. Dann steigt gegebenenfalls auch die Bereitschaft zu investieren“, ergänzt Mabire.

Cybersecurity muss auch für kleinere Flotten erschwinglich sein

Generell gilt die Faustformel: Je größer das Unternehmen, desto größer ist auch das Bewusstsein für Probleme der Cybersecurity. „Es existiert eine Cybersecurity-Kluft zwischen den wenigen großen Playern und einer Vielzahl kleinerer Unternehmen. Während die Konzerne Strategien entwickeln, IT-Spezialisten anheuern und eigene Cybereinheiten aufstellen, fehlen kleineren Betriebe oft die finanziellen Mittel dazu und auch der Fokus auf das Thema“, so Mathias Dehm. Das sei gerade in der margenschwachen Logistikbranche, wo jeder Cent für eine Investition umgedreht werden muss, ein Problem. Tatsächlich ist die Branche laut der letzten Erhebung des Bundesamtes für Güterverkehr ganz überwiegend von klein- und mittelständischen Unternehmen geprägt.[[1]](#footnote-2) Neben gesetzlichen Regelungen wird es darauf ankommen, den Unternehmen, insbesondere kleineren, bezahlbare Lösungsangebote zu machen, die sich noch stärker auf deren Bedürfnisse einstellen. „Keine Frage: Cybersicherheit muss für alle erschwinglich sein“, sagt Ido Ben Ami, der die Forschung und Entwicklung bei Argus Cyber Security leitet. „Aus diesem Grund gibt es skalierbare Cybersecurity-Lösungen, die es kleineren Flotten ermöglichen, ihre Cybersecurity-Kapazitäten zu erweitern, während sie wachsen. So kann zum Beispiel ein Security Operations Center, das es Flottenmanagern erlaubt Angriffe zu überwachen, zu erkennen und darauf zu reagieren, auf die spezifischen Anforderungen und Ressourcen jeder Organisation zugeschnitten werden.“

Cybersicherheit erfordert ganzheitliche Sicht auf das Unternehmen

Sofern es Investitionen in Cybersecurity gibt, tun sich viele Unternehmen beim nachhaltigen Einsatz der Sicherheitslösungen schwer, denn Software wird bisweilen mit der Programmierung als abgeschlossen betrachtet. Doch um die Systeme aktuell zu halten, bedarf es kontinuierlicher Investitionen – etwa in die Anpassung in die Systemumgebung des eigenen Unternehmens, regelmäßige Updates, Schulungen der Mitarbeiter und nicht zuletzt in den Support. Kurzum: Eine Einmalinvestition reicht nicht aus, um das Thema umfassend anzugehen und dauerhaft im Unternehmen zu verankern. „Neben den Trucks an sich betrifft Cybersecurity auch die gesamte IT inklusive der Flottenmanagementsysteme oder auch die Arbeitsorganisation. Diese Verantwortungsbereiche sollten möglichst in einem ganzheitlichen Konzept zusammengeführt werden, damit alle Schnittstellen zwischen den Bereichen abgedeckt werden“, gibt Matthias Dehm von Continental zu bedenken.

Mehr Fahrzeugsicherheit durch einheitliche Cybersecurity-Standards

In den vergangenen drei Jahren wurde an einer neuen Regulierung gearbeitet, um einheitliche Cybersicherheitsstandards für Fahrzeuge zu etablieren. Die von der Arbeitsgruppe WP.29 der UN-Wirtschaftskommission (UN ECE) ausgearbeitete Regulierung prüft die Sicherheitsvorgaben während der Fahrzeugtypenzulassung. Neben der Überprüfung, ob die eingesetzten Sicherheitsmaßnahmen angemessen sind, werden unter anderem auch die Unternehmensprozesse auditiert. So wird sichergestellt, dass Cybersecurity bei der Entwicklung und Industrialisierung von Komponenten und Software berücksichtigt wird. Die UN ECE WP.29 Regulierung wird ab Mitte 2022 schrittweise eingeführt und gilt ab Juli 2024 für alle neu zugelassenen Fahrzeugtypen in Europa – ein wichtiger Schritt für mehr Fahrzeugsicherheit. „Cybersecurity wird mit der immer stärkeren Vernetzung – etwa beim Automatisierten Fahren und Anwendungen rund um 5G weiter an Bedeutung gewinnen und sollte bei neuen Anwendungsbereichen daher immer mitgedacht werden“, so Gilles Mabire.

Über die Studie

Für die Studie „Digitalisierung und Cybersecurity in der Nutzfahrzeugbranche“ hat das infas Institut für angewandte Sozialwissenschaft im Auftrag von Continental Experten in Verbänden, Behörden, Speditionen und Technologiedienstleistern zu den Herausforderungen in der Transport- und Logistikbranche durch die Digitalisierung und Cybersicherheit befragt. Die insgesamt zehn qualitativen Leitfadeninterviews wurden zwischen Dezember 2019 und Februar 2020 in offener Form per Telefon oder persönlich geführt. Es ging um Fragen zur Digitalisierung im Unternehmen sowie um die Bedeutung von Cybersecurity, Bedrohungen, Maßnahmen, Strukturen sowie um Verbesserungsbedarfe und Wünsche. Ergänzt wurde die Befragung durch ein Branchenpanel, für das infas im Straßengüterverkehr tätige Unternehmen, Logistiker und Spediteure online befragt hat. Dafür wurden mittels statistischer Zufallsauswahl zwischen Februar und Mai Transportunternehmen, Logistiker und Spediteure in Deutschland kontaktiert. Die Ergebnisse der insgesamt 40 Teilnehmer liefern einen Einblick zum Stand der Digitalisierung der Branche, zum Einsatz von Softwarelösungen sowie zum Thema Cybersecurity im Nutzfahrzeugbereich.

Continental entwickelt wegweisende Technologien und Dienste für die nachhaltige und vernetzte Mobilität der Menschen und ihrer Güter. Das 1871 gegründete Technologieunternehmen bietet sichere, effiziente, intelligente und erschwingliche Lösungen für Fahrzeuge, Maschinen, Verkehr und Transport. Continental erzielte 2019 einen Umsatz von 44,5 Milliarden Euro und beschäftigt aktuell mehr als 232.000 Mitarbeiter in 59 Ländern und Märkten.

Continental entwickelt innovative Technologien für mehr Sicherheit, Effizienz und Vernetzung im Güterverkehr. Die Produkte und Dienstleistungen des Unternehmens bieten Herstellern von Nutzfahrzeugen und dem dazugehörigen Ersatzteilmarkt einen messbaren Nutzen. Sie profitieren von einem breit gefächerten Angebot und voll integrierten Systemen. Das Portfolio umfasst Reifen, digitale Reifenüberwachung, Flottenmanagementlösungen, Tachographen, Schläuche, Luftfedern, Lösungen für Antriebsstrang und Abgasnachbehandlung, elektronische Steuergeräte, Displays, Sensoren, Fahrerassistenzsysteme, cloudbasierte Anwendungen sowie eHorizon-Anwendungen und -Karten. Im Jahr 2019 erzielte Continental mit Produkten, Systemen und Services für den Nutzfahrzeugbereich einen weltweiten Umsatz von 5 Milliarden Euro.

**Kontakt für Journalisten**

Christopher Schrecke

Leiter Externe Kommunikation

Commercial Vehicles & Services

Continental

Telefon: +49 69 7603-2022

E-Mail: christopher.schrecke@continental-corporation.com

**Presseportal:** www.continental-presse.de

**Mediathek:** www.continental.de/mediathek

**Bilder und Bildunterschriften**

|  |  |
| --- | --- |
| Continental\_PP\_Studie\_Cybersecurity\_Infographik I\_Secure\_DE.jpg | Die Nutzfahrzeugindustrie fühlt sich relativ sicher in Bezug auf die Cybersicherheit und investiert daher zurückhaltend – eine Vorgehensweise, die Risiken bergen kann. |
| Continental\_PP\_Studie\_Cybersecurity\_Infographik II\_SW Update\_DE.jpg | Die meisten Fuhrparkunternehmen vertrauen auf Hersteller und Werkstattbesuche, wenn es um die Aktualität der Software geht. Nur wenige haben einen zentralen Überblick, ob die Fahrzeug-Software aktuell ist.  |
| Continental\_PP\_CV\_Cybersecurity\_wAttacks.jpg | Die neue UN ECE Regulierung WP.29 schafft erstmals einheitliche Cybersecurity-Standards für Fahrzeuge. Darüber hinaus können stärker auf die branchentypischen kleineren Unternehmen zugeschnittene Lösungen mehr Fahrzeugsicherheit bringen. |

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