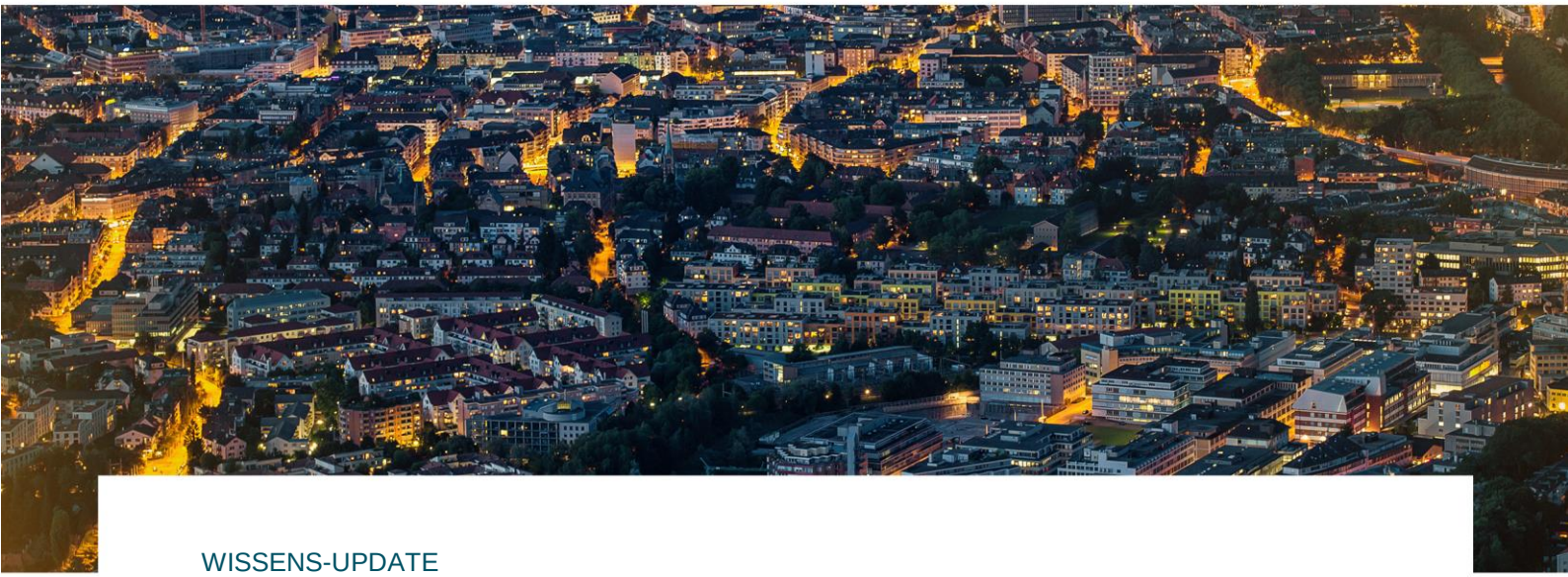
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

Sicher vernetztes Flottenmanagement spart Aufwand, Zeit und Geld

Patrick Bucher | Sales Manager IoT Security | Steinhausen, 26. April 2022

Die Logistikbranche gehört zur Speerspitze der industriellen Digitalisierung – nicht nur im Bereich der Lagerbewirtschaftung. Auch beim Flottenmanagement können Transportunternehmer dank neuer Technologien ihre Effizienz steigern und Mehrwert schaffen. Vorausgesetzt, die Cyber Security ist gewährleistet.

Bei grossen Handelshäusern wie Amazon oder bei Betrieben wie der Post zeigt sich: Der technologische Wandel in der Logistik ist rasant, die Branche gehört zur Avantgarde der Digitalisierung. RFID Tracking, Warencodes, mobile Terminals, Sensoren, Robotik und IT-Umgebung sind zu einem smarten System zusammengewachsen.

Das Internet der Dinge (IoT) revolutioniert allerdings nicht nur den Bereich der Lagerung und Sortierung, sondern auch den Bereich des Transports. Hierbei nimmt das Flottenmanagement eine zentrale Rolle ein. Vernetzte Fahrzeuge, die mit Trackern unterschiedlichste Daten sammeln und an eine zentrale Plattform senden, sorgen für mehr Transparenz, können die Effizienz eines Logistikbetriebs markant steigern und zudem als Basis dienen für neue Businessmodelle.

IoT-Vernetzung bringt Vorteile und Mehrwert

Naheliegend ist der Vorteil eines IoT-basierten Flottenmanagements bei der Einsatzplanung: Digitale Tracking-Lösungen erlauben es einem Logistikunternehmen nicht nur, jederzeit zu wissen, wo sich seine Fahrzeuge gerade befinden oder wie schnell und wie lange sie schon unterwegs sind. Basierend auf Informationen zu Gütern und Bestimmungsort lassen sich auch Auslastung und Performance der Fahrzeuge optimieren. Werden Güter verschiedener Auftraggeber transportiert, ermöglicht ein intelligentes Tracking zudem, die Kosten für den Transport aufwand- und verursachergerecht abzurechnen. Gekoppelt mit Daten zu Verkehrsaufkommen, Baustellen und Staus können vernetzte Systeme die Routen in Real-Time der Situation auf der Strasse anpassen – ohne dass sich ein Disponent stundenlang darüber Gedanken machen muss. Das alles spart Aufwand, Zeit, Treibstoff und damit Geld.

Werden auch Serviceinformationen ins IoT-System integriert, schafft das weiteren Mehrwert. Das Logistikunternehmen kann sofort handeln, falls ein Fahrzeug technische Probleme hat. Zudem ermöglichen die Daten zu Fahrzeugzustand und Nutzung auch eine optimale Vorbereitung von Wartung und Reparatur. Service-Intervalle können so geplant werden, dass die Ausfallzeiten so kurz wie möglich sind oder während auftragsschwächeren Zeiten stattfinden. Das Zusammenspiel und die intelligente Auswertung der gesammelten Informationen kommen schliesslich auch den Kundinnen und Kunden zugute: Sie sind jederzeit darüber informiert, wann eine Lieferung bei ihnen eintreffen wird. Das wiederum erhöht die Zufriedenheit, schafft Vertrauen und Kundenbindung für das Logistikunternehmen und seine Auftraggeber.

Erfolgsfaktor: Schutz der Daten vor Cyber-Kriminellen

Verschiedene Anspruchsgruppen versprechen sich eine Vereinfachung der Prozesse und mehr Transparenz durch den Zugriff auf die Daten – nicht nur das Logistikunternehmen und seine Kunden, sondern seit der Einführung des intelligenten Fahrtenschreibers im Juni 2019 auch Behörden wie die Zollverwaltung und ihre Zulassungsstelle für die Schwerverkehrsabgabe LSVA. Hinzu kommen die Auftraggeber und Hersteller der transportierten Waren sowie Fahrzeug-Servicedienstleister.

Die Operational Technology (OT) des Logistikunternehmens, wo die Daten zusammenfliessen, wird dadurch zur Drehscheibe für all diese Stakeholder; ein komplexes IoT-Ökosystem entsteht. Bei allen Vorteilen bringt ein vernetztes System auch Sicherheitsrisiken mit sich. Die Daten werden auf verschiedenen Kanälen an die Anspruchsgruppen gesendet. Mehrere Gruppen stellen Anspruch auf dieselben Sensordaten (z.B. die GPS-Position oder den Zugriff auf den CAN Bus der Motorsteuerung).

Hierbei gilt es in einem ersten Schritt sicherzustellen, dass jeder nur Einsicht in diejenigen Daten erhält, die für ihn relevant sind. Denn Informationen über Position, Service, Produktivität und zeitliche Überwachungen haben einen Wert, der adäquat geschützt werden muss. Der Kunde, der auf seine Lieferung wartet, braucht keine Informationen zur Ankunftszeit anderer Lieferungen, der Auftraggeber muss keinen Zugriff auf die Abrechnung der Schwerverkehrsabgabe haben, die vorgesehenen Wartungsintervalle gehen die Zollverwaltung wenig an.

In einem zweiten Schritt muss garantiert werden, dass die Verbindungen, mit denen Daten übertragen werden, sicher sind und nicht zum Angriffspunkt für Cyber-Kriminelle werden. Es braucht folglich funktionierende Sicherheitsmassnahmen, die ein Eindringen ins Fahrzeug- und Logistiksystem durch die vernetzten Umsysteme verhindern. Szenarien, in denen Erpressungsversuche verübt werden können, welche die Cloud des Logistikbetreibers nutzen, um an Sicherheitsfunktionen eines Fahrzeugherstellers zu kommen, müssen per Design verhindert werden können.

Sicherheit muss bei Herstellern und Betreibern im Fokus stehen
Hersteller und Anwender sind bei der Gewährleistung der IoT Security gleichermassen gefordert. Hersteller von Trackinglösungen oder Fahrzeugen müssen ihre Technologie mit sicheren Schnittstellen ausrüsten und eine Sicherheitsarchitektur bereits im Rahmen der Geräteentwicklung berücksichtigen – «Security by Design» also.

Anwender wiederum sind angehalten, Sicherheitsrisiken bei der Integration neuer Lösungen in die bestehende IT-Umgebung zu minimieren. Die Herausforderung besteht darin, dass die Sicherheitsarchitektur einer effizienten Nutzung der Daten nicht im Weg steht. Denn nur wenn die Informationen in Echtzeit abrufbar und einfach zugänglich sind, entfaltet sich ihr ganzes Business-Potenzial. Auch die Flexibilität der Technologie, sich veränderten Netzwerkumgebungen oder Aufgabenfeldern anzupassen, darf durch die Sicherheitsvorkehrungen nicht eingeschränkt werden.

CyOne Security ist der kompetente Partner für die IoT Security im Flottenmanagement
Damit die sichere Integration von IoT-Geräten effizient klappt, lohnt es sich, im Bereich Flottenmanagement mit einem versierten IoT Security-Experten wie der CyOne Security zusammenzuarbeiten. Die CyOne Security kann tiefes Expertenwissen in Cipher und Cyber Security in die IoT-Sicherheitskonzepte von Logistikunternehmen einbringen und die Sicherheitsbetrachtungen bei der Lösungskonzeption oder der Wahl in Bezug auf die Qualität der Sicherheitsfunktionen der Hersteller unterstützen.

Dabei wird die Sicherheit der einzelnen Komponenten, wie zum Beispiel der GPS Tracker, die Sicherheit des Systems, z.B. das Tracking, im Zusammenspiel sowie dessen Betrieb berücksichtigt. Aus Product Security, System Security und Operational Security entsteht eine 360°-Sicherheitskompetenz.

Sowohl für Hersteller als auch für Anwender prüft die CyOne Security bestehende Komponenten sowie die Sicherheitsarchitektur des Gesamtsystems und spürt mögliche Schwachstellen auf. Das Expertenwissen kommt auch beim Design einer grundlegend neuen Sicherheitsarchitektur für das Flottenmanagement und die IT-Umgebung des Unternehmens zum Tragen. Schliesslich kann die CyOne Security als Dienstleisterin sowohl für Hersteller als auch für Anwender sichere Update-Plattformen betreiben. Damit das vernetzte Flottenmanagement nicht nur heute, sondern auch in Zukunft sein Potenzial entfalten kann.

Beginnen Sie heute und schützen Sie Ihr Flottenmanagement vor Cyber-Risiken.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren IoT Security-Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse Ihres Flottenmanagements, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.