Neue Cybersicherheits- und Softwareupdatestandards in der Automobilbranche

Ein Beitrag von Daniel Wuhrmann, Thorsten Deeg und Stefan Hessel

Die durch das Weltforum für die Harmonisierung von Fahrzeugvorschriften (WP.29) als Arbeitsgruppe der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE) erarbeiteten Regelungen wurden durch Veröffentlichung am 9. März 2021 im Amtsblatt auf europäischer Ebene verbindlich umgesetzt. Damit liegt auf europäischer Ebene erstmals ein verbindliches und einheitliches Regelungssystem hinsichtlich der Cybersicherheit und Softwareupdates im Automobilsektor vor.

Bedingt durch die zunehmende Vernetzung und Digitalisierung von Fahrzeugen in den vergangenen Jahren ist auch das potenzielle Risiko von Cyberangriffen auf diese gestiegen. Mit den neuen Regelungen soll nun den steigenden Risiken entgegengetreten werden.

Kernbestandteile der neuen Regelungen sind die Verpflichtung zur Einführung eines Managementsystems für Cybersicherheit im Fahrzeug und die Schaffung eines Rechtsrahmens für Updates aus der Ferne (Over-the-Air- oder OTA-Updates). Da diese neuen Regularien deutlich über die bisherigen Anforderungen in Sachen Cybersicherheit bei Fahrzeugen hinausgehen, sollten sich Hersteller von Fahrzeugen und deren Zulieferer umgehend auf diese Neuerungen einstellen.

Anforderungen hinsichtlich Cybersicherheit

Hersteller werden zur Etablierung eines Cybersicherheitsmanagementssystems (CSMS) verpflichtet. Dieses bezeichnet nach Ziffer 2.3 der UN-Regelung Nr. 155 einen systematischen, risikobasierten Ansatz zur Festlegung von organisatorischen Abläufen, Zuständigkeiten und Governance beim Umgang mit Risiken im Zusammenhang mit Cyberbedrohungen für Fahrzeuge und beim Schutz von Fahrzeugen vor Cyberangriffen. Das CSMS ist Voraussetzung für eine Genehmigung des Fahrzeugtyps nach Ziffer 5 der UN-Regelung Nr. 155.

Hersteller entsprechender Fahrzeuge sollten daher unter anderem Folgendes gewährleisten:

- Etablierung und Verfügbarkeit eines CSMS
- Durchführung einer Risikoanalyse für Cybersicherheit und Identifikation kritischer Risiken über die gesamte Lieferkette hinweg
- Risikobewertung
- Implementierung geeigneter Cybersicherheitsmaßnahmen zur Identifizierung und Verhinderung von Cyberangriffen
- Fortlaufende Überwachung typenspezifischer Cybersicherheitsvorfälle

Da die Hersteller die gesamte Lieferkette zu überprüfen haben, werden auch mittelbar Zulieferer den Anforderungen unterworfen, da sie oftmals mit der Herstellung der einzelnen Komponenten, die den Cybersicherheitsanforderungen entsprechen müssen, betraut sind.

Anforderungen hinsichtlich Software-Updates

Eng verknüpft mit den Vorgaben für ein CSMS ist die neue UN-Regelung zur Etablierung eines Softwareaktualisierungsmanagements. Dies bezeichnet nach Ziffer 2.5 der UN-Regelung Nr. 156 einen systematischen Ansatz zur Festlegung organisatorischer Verfahren und Vorgänge, um den Anforderungen an die Bereitstellung von Softwareaktualisierungen zu gemäß dieser Regelung zu entsprechen. Dadurch soll gewährleistet werden, dass Hersteller in der Lage sind, erkannte Sicherheitslücken oder Schwachstellen wirksam und aus der Ferne zu schließen.

Im Einzelnen haben die Hersteller daher folgende Verpflichtungen zu erfüllen:

- Etablierung und Verfügbarkeit eines Softwareaktualisierungsmanagementsystems für Fahrzeuge im Straßenverkehr
- Verfahren zur Identifizierung der Zielfahrzeuge sowie Kompatibilität des Zielfahrzeugs mit der Konfiguration
- Bei OTA-Updates: Wiederherstellungsfunktion bei fehlgeschlagenen Updates, Updates nur bei ausreichender Stromversorgung, Gewährleistung einer sicheren Ausführung (auch während der Fahrt), Information des Nutzers über jedes Update und dessen erfolgreiche Installation, Prüfung zur Durchführbarkeit des Updates vor dessen Installation, Information des Nutzers über die Notwendigkeit eines Werkstattbesuchs

Fazit und weitere Schritte vonseiten der Hersteller

Aufgrund der neuartigen und erstmals verbindlichen Regelungen der UN stehen Hersteller und Zulieferer vor besonderen Herausforderungen. Diese neuen verbindlichen Regelungen machen deutlich, dass das Thema Cybersicherheit auch in der Automobilbranche zunehmend reguliert wird und sich der Rechtsrahmen verengt. Die zunehmende Digitalisierung von Fahrzeugen soll keine Angriffsflächen für Cyberattacken bieten. Daher ist gut beraten, wer sich bereits frühzeitig mit den neuen Anforderungen auseinandersetzt und Prozesse für Cybersicherheit by design schafft und mit der flächendeckenden Implementierung von Verteidigungsstrategien beginnt.

[März 2021]

Unternehmenskontakt: Melanie Schaumann I Head of Marketing & Communications I T > +49 30 / 2332895 0 I E melanie.schaumann@reuschlaw.de