Autozulieferer und Ladenetz Einfallstor für Hackerangriffe

Vernetzte Fahrzeuge bieten enorme Möglichkeiten, bergen aber auch Gefahren

Autos und Autoindustrie werden nach einer Studie des Branchenexperten Stefan Bratzel zunehmend Ziel von Hackerangriffen. Die Ladeinfrastruktur für Elektrofahrzeuge gehöre zu den besonders gefährdeten Bereichen: Sie sei durch die „verschiedenen Marktteilnehmer außerordentlich komplex und bietet grundsätzlich viele Angriffspunkte für Cyber-Kriminelle", heißt es in der am Dienstag vom CAM-Institut in Bergisch Gladbach veröffentlichten Studie.

Ein weiteres Einfallstor seien Zulieferer: „Die komplexe Lieferkette gilt als große Schwachstelle und bietet zentrale Angriffspunkte, die mit hoher Wahrscheinlichkeit und oft großem Schadensausmaß ausgenutzt werden."

Das Risiko wächst

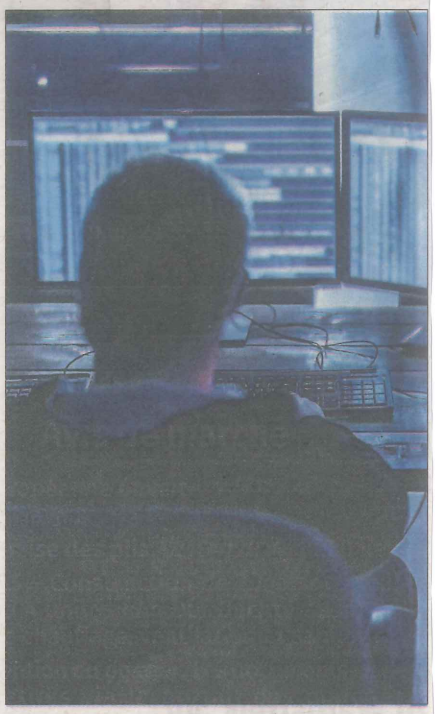
Mit zunehmender E-Mobilität, Digitalisierung und Vernetzung der Fahrzeuge sowie der Produktion und Logistik wachse das Risiko. Umfassende Cybersicherheitsstrategien seien dringend notwendig, allerdings auch sehr aufwendig. „Die Unternehmen unterscheiden sich jedoch bezüglich der Qualität von Konzeption und Umsetzung erheblich", sagte Bratzel.

Bei vielen Zulieferern und Dienstleistern seien sie noch auf niedrigem Niveau. Kundenwünsche nach Connected Cars und Connected Services erzeugten einen enormen Wettbewerbsdruck, durch den Sicherheitsaspekte mitunter in den Hintergrund gerieten. Mit zunehmender Vernetzung und Automatisierung der Lieferkette wachse die Angriffsfläche.

Zahl der Angriffe wächst

Die Menge und Qualität der Angriffe sei in den letzten Jahren erheblich gestiegen, heißt es in der Studie, die das CAM-Institut im Auftrag des kalifornischen IT-Konzerns Cisco erstellt hat. So habe Toyota den Betrieb seiner japanischen Fabriken 2022 kurz aussetzen müssen, weil ein Zulieferer von Kunststoffteilen und elektronischen Komponenten von einem mutmaßlichen Cyber-Angriff getroffen wurde.

Bei General Motors, Continental und Moovit hätten Cyber-Kriminelle Daten gestohlen. „Im März 2023 wurde von einem Cyber-Angriff auf Tesla berichtet, bei dem sich Hacker aus der Ferne in ein Fahrzeug einwählen und diverse Funktionen ausführen konnten. Dazu zählten etwa die Betätigung der Hupe, das Öffnen des Kofferraumes, das Einschalten des Abblendlichts sowie die Manipulation des Infotainment-Systems." *dpa*



Zunehmend geraten auch vernetzte Fahrzeuge ins Visier der Hacker. Foto: Getty Images