
© Escrypt

**Dr.-Ing. Thomas Wollinger**
ist Geschäftsführer von Escrypt

# Drei gute Gründe für V-to-X-Security

Die V-to-X-Kommunikation rollt an und mit ihr eine neue Dimension von Sicherheitsanforderungen auf uns zu. V-to-X wird die Angreifbarkeit von vernetzten Fahrzeugen auf eine neue Stufe heben. Die Angriffsfläche wird geradezu explodieren und mit ihr die Anziehungskraft für Cracker und Hacker. Ist der Cyberangriff auf ein einzelnes Fahrzeug heute nur wenig attraktiv, so birgt eine mögliche konzertierte Attacke auf viele vernetzte Fahrzeuge und deren Infrastruktur in Zukunft ganz andere Erlös- und Wirkungschancen für Cyberkriminelle.

Keine Frage also: Vernetztes Fahren braucht IT-Security, ganzheitlich angelegt, dauerhaft wirksam, über alle Fahrzeuge und Verkehrsteilnehmer, alle Kommunikations- und Infrastrukturkomponenten hinweg. Konkret sehe ich mindestens drei gute Gründe für all jene, die vernetztes Fahren künftig mitgestalten wollen, sich heute intensiv mit V-to-X-Security zu befassen: Schutz von Menschen und Daten (Safety und Privacy), Zugang zum Markt und Erlangung von Rechtssicherheit. In anderen Worten: Die Absicherung der V-to-X-Kommunikation ist eine ethische, eine ökonomische und eine rechtliche Notwendigkeit.

Der erste Grund: Der Schutz der Privatsphäre und Unversehrtheit der Menschen ist unverhandelbar. Im gleichen Maße wie wir einen V-to-X-Datenaustausch befördern, müssen wir die privaten Daten der Verkehrsteilnehmer vor unberechtigtem Zugriff schützen. Fast noch dringlicher müssen wir Fahrzeuge und Infrastruktur vor Manipulation schützen. Dass Hacker per V-to-X das Kommando über Fahrzeuge oder Verkehrsanlagen übernehmen, ist bekanntlich das ultimative Schreckensszenario.

Grund Nummer Zwei: Marktzugang. Wer teilhaben möchte an der wegweisenden Technologie des vernetzten Fahrens: Autobauer und ihre Zulieferer, Hersteller von Roadside Equipment, Betreiber von Verkehrsinfrastruktur oder Fahrzeugflotten wird V-to-X-Security zwingend mit einbringen müssen. Sie ist Voraussetzung für jedes Geschäftsmodell, das auf V-to-X-Kommunikation fußt. V-to-X-Security ist also kein Wettbewerbsfaktor, sondern schlichte Vorbedingung für den Zugang zum Zukunftsmarkt des vernetzten Fahrens.

Dritter wichtiger Grund für V-to-X-Security: Rechtssicherheit. Die US-Legislative ist bereits dabei, einen Rechtsrahmen für autonomes und vernetztes Fahren zu schaffen. Andere werden nachziehen. Denn spätestens, wenn zum ersten Mal ein Fahrzeug per V-to-X gehackt wird, stellt sich die Schuld- und Haftungsfrage. Deshalb muss V-to-X-Kommunikation heute schon mögliche gesetzliche Security-Anforderungen in den Blick nehmen.

Vernetztes Fahren wird für uns alle ein Zugewinn sein. Doch nur ausreichend abgesichert gegen Angriffe, Manipulation und Datendiebstahl wird es die nötige gesellschaftliche Akzeptanz finden. Wir möchten die neuen Technologien guten Gewissens zur Verfügung stellen, und wir möchten sie selbst angstfrei nutzen können. Kümmern wir uns gemeinsam darum, dass es gelingt.