

Inhalt

1 Einleitung	9	3.2.1 Basis-Angriffe und ihre Kombinationen	45
1.1 Motivation/Zielstellung	9	3.2.2 Angreiferspektrum nach CERT	46
1.2 Vorgehensweise	9	3.2.3 Wesentliche Angreiferklassen elektronischer Veränderungen an Fahrzeug- und Infrastruktursystemen	47
1.3 Überblick über den vorliegenden Schlussbericht	10	3.3 Aufbereitung der Rechercheergebnisse nach Angreiferwissen	49
1.4 Einleitende Begriffsklärungen und Konventionen	11	3.4 Abschließende Abschätzung zur Relevanz der Schwachstellen	50
1.4.1 Klärung der hier vorgenommenen Verwendung des Veränderungsbegriffs	11	4 Abschätzung des potenziellen Risikos durch Bewertung der Auftrittswahrscheinlichkeit elektronischer Veränderungen	52
1.4.2 Aspekte der Sicherheit	11	4.1 Bewertung der Auftrittswahrscheinlichkeit aus der Risikoanalyse als Kombination der Abschätzungen für Bedrohungslage und Schwachstellen	53
1.4.3 Ableitung von Komponentenklassen aus automotiven Domänen	12	4.2 Verifikation und Ergänzung der tabellarischen Risikobewertung	54
1.4.4 Überblick Fahrzeug IT und -Netze	13	4.2.1 Informationen von Experten	54
2 Abschätzung der Bedrohungslage: Recherche zur elektronischen Veränderung von Kfz- und Infrastruktursystemen	14	5 Abschätzung potenzieller Gefahren aus elektronischen Veränderungen	56
2.1 Analyse der Bedrohungslage: Recherche zu veränderten Komponenten	14	5.1 Vorbetrachtungen zur Gefahrenanalyse	56
2.1.1 Kfz-Systeme als Ziel elektronischer Veränderungen	14	5.1.1 Berücksichtigung von Einbußen in Komfort, Security und Safety	56
2.1.2 Infrastruktursysteme als Ziel elektronischer Veränderungen	35	5.1.2 Unterscheidung von direkten Auswirkungen und potenziellen Nebeneffekten	58
2.2 Systematisierung: Aufbereitung der Rechercheergebnisse nach Komponentenklassen	38	5.1.3 Das allgemeine Spektrum von Gefahren im Automobilbereich	60
2.3 Abschließende Abschätzung zur Bedrohungslage	40	5.2 Abschätzung der Gefährdung für den Straßenverkehr	64
2.3.1 Berücksichtigte Kenngrößen	40	5.2.1 Recherche zu praktischen Vorkommnissen entsprechender Gefährdungssituationen bzw. Gefahren	65
2.3.2 Ergebnis der Abschätzung	41	5.3 Abschließende Abschätzungen zu Gefährdungen aus elektronischen Veränderungen	72
3 Abschätzung ausgenutzter Schwachstellen unter Einbeziehung des Angreiferspektrums	43		
3.1 Definition exemplarischer Schwachstellenkategorien	44		
3.2 Untersuchung des Angreiferspektrums	45		

6	Potenzielle Entwicklungen in naher Zukunft	74
6.1	Übersicht über exemplarisch ausgewählte Forschungsprojekte zu C2X	75
6.2	Simulation eines hypothetischen Angriffsszenarios: Wurm-Epidemien in C2C-Netzen	76
6.3	Diskussion im Kontext zukünftiger Fahrerassistenzsysteme	79
7	Einschätzung der Ergebnisse	79
7.1	Fazit zum Gefährdungspotenzial: Subsumierung ausgewählter potenzieller Gefahren mit besonderer Relevanz für den Straßenverkehr	80
7.1.1	Exemplarische Gefahren nach Veränderungen zur Leistungssteigerung	80
7.1.2	Exemplarische Gefahren nach Veränderungen an der Servolenkung	81
7.1.3	Exemplarische Gefahren nach Veränderungen zum elektronischen Tieferlegen	82
7.1.4	Exemplarische Gefahren nach Veränderungen am Airbagsystem	82
7.1.5	Exemplarische Gefahren nach Veränderungen am Wegstreckenzähler	82
7.1.6	Exemplarische Gefahren nach Veränderungen zur Warnung vor Geschwindigkeitsmesseinrichtungen	82
7.1.7	Exemplarische Gefahren nach Veränderungen für TV/Video in Motion	83
7.1.8	Exemplarische Gefahren nach unsachgemäßer Nachrüstung von Xenon-Scheinwerfern	84
7.2	Fazit und Folgerungen für die Zukunft	84
8	Kompaktübersicht Rechercheergebnisse	86
	Literatur	87