

Inhaltsverzeichnis

Einleitende Informationen.....	29
Teil A: Grundlagen.....	33
1 Internet und Co.....	35
1.1 Arpanet	35
1.2 Internet und World Wide Web	36
1.3 Deep Web und Darknet.....	36
1.4 Internet of Things.....	37
2 Hacker und ihre Motivation	39
2.1 Vorsicht: Falschmeldung	39
2.2 Gut gegen Böse	40
2.3 European Cybersecurity Skills Framework (ECSF)	43
2.4 Die Hackerparagrafen (§ 202 und § 303 StGB)	44
2.5 Chaos Computer Club	46
2.6 Anonymous	47
2.7 Staatliche Hackergruppen und APTs.....	48
2.8 Ein Blick zurück	50
2.9 Alle Ampeln auf GRÜN.....	52
3 Instanzen und Regelwerke	55
3.1 Verordnungsgeber.....	55
3.2 Institutionelle Instanzen	55
3.2.1 Einleitende Informationen	55
3.2.2 Deutsche Instanzen.....	56
3.2.3 Europäische Instanzen.....	59
3.2.4 Amerikanische Instanzen	61
3.2.5 Internationale Instanzen.....	64
3.3 Regelwerke und Gesetze	65
4 Schwachstellen und Sicherheitslücken.....	69
4.1 Common Weakness Enumeration (CWE)	69
4.2 Common Vulnerabilities and Exposures (CVE)	71
4.3 Known Exploited Vulnerabilities Catalog (KEV)	73
4.4 Common Vulnerability Scoring System (CVSS).....	73
4.5 Open Worldwide Application Security Project (OWASP).....	74
4.6 Cybersicherheitswarnungen (CSW) des BSI.....	74

5	Malware und Hacker-Tools	75
5.1	Malware	75
5.1.1	Viren und Würmer	75
5.1.2	Trojaner	76
5.1.3	Ransomware	77
5.1.4	Adware	77
5.1.5	Spyware	78
5.1.6	Rootkits	78
5.1.7	Dateilose Malware	78
5.2	Angriffswerkzeuge und Cyberwaffen	78
5.2.1	Kali Linux	78
5.2.2	Werkzeuge zum Hacken kabelloser Netzwerke	80
5.2.3	Schwachstellenscanner	80
5.2.4	Passwort-Cracker	81
5.2.5	Netzwerkanalyse-Tools	82
5.2.6	Wiper	83
6	Angriffsvektoren	85
6.1	Was ist ein Angriffsvektor?	85
6.2	Indirekte Angriffsvektoren	85
6.2.1	Desinformation und Täuschung	85
6.2.2	Social Engineering	86
6.2.3	Reverse Engineering	87
6.2.4	Watering-Hole-Angriffe	88
6.2.5	Supply-Chain-Angriffe	88
6.2.6	Manipulation von Software-Updates	88
6.2.7	DNS-Spoofing	89
6.2.8	Einsatz von Botnets	89
6.2.9	Einsatz generativer KI/Prompt Injection	90
6.3	Direkte Angriffsvektoren	91
6.3.1	Ransomware-Angriff und Data Exfiltration	91
6.3.2	Injection-Angriffe	92
6.3.3	Angriffe auf die Authentifizierung	92
6.3.4	Angriffe auf Netzwerke	93
6.3.5	Denial-of-Service-(DoS-)Angriffe	94
6.3.6	Angriffe auf Application Programming Interfaces (APIs)	94
6.3.7	Angriffe auf Steuergeräte-Hardware	95
7	Minderungsmaßnahmen zur Erhöhung der Cybersecurity	97
7.1	Minderungsstrategien	97
7.1.1	Auswirkung eines Angriffs wird verhindert	97
7.1.2	Auswirkung eines Angriffs wird erkannt	98
7.2	Festlegung von Legenden für Darstellungen	98
7.3	Definitionen von Schlüsselbegriffen	100
7.3.1	Dokumente, Daten und Dateien	100
7.3.2	Sicherheit	101

7.3.3	Integrität	101
7.3.4	Authentizität	101
7.3.5	Autorisierung	102
7.3.6	Vertraulichkeit von Daten	103
7.4	Verfahren zur Herstellung und Prüfung der Integrität von Daten	103
7.4.1	Anerkannte Integritätsmerkmale	103
7.4.2	Integrität der Daten <u>in</u> einem System	105
7.4.3	Integrität bei der Übermittlung von Daten zwischen Systemen	107
7.4.4	Grenze der Zuverlässigkeit von Integritätsmerkmalen	109
7.5	Verfahren zur Herstellung der Authentizität von Daten	110
7.5.1	Symmetrische kryptografische Verfahren	111
7.5.2	Asymmetrische kryptografische Verfahren	113
7.5.2.1	Generierung eines Schlüsselpaars	113
7.5.2.2	Signieren und Signaturprüfung	114
7.5.2.3	Authentizität des öffentlichen Schlüssels	115
7.6	Verfahren zur Authentifikation von Entitäten	117
7.6.1	Authentifikation an einem System	117
7.6.1.1	Authentifikation einer Entität an einem System	117
7.6.1.2	Authentifikation mit Einbindung einer dritten definierten Instanz	119
7.6.2	Authentifikation einer Entität im Rahmen der Datenübermittlung	120
7.7	Verfahren zur Herstellung der Vertraulichkeit von Daten	121
7.7.1	Symmetrische kryptografische Verfahren	121
7.7.2	Asymmetrische kryptografische Verfahren	123
7.7.3	Hybrides Verfahren zur Performanceoptimierung	125
7.8	Geheimnis- und Schlüssel-Management	126
7.8.1	Entropie von Geheimnissen und Zufallszahlen	126
7.8.2	Generierung von Geheimnissen	128
7.8.2.1	Unbefristete Geheimnisse	128
7.8.2.2	Befristete Geheimnisse	129
7.8.2.3	Andere Einschränkungen der Nutzung von Geheimnissen	129
7.8.3	Geheimnisträger	129
7.8.3.1	Eigene Geheimnisse	129
7.8.3.2	Vereinbarung und Umgang mit <u>as</u> ymmetrischen Schlüsseln	130
7.8.3.3	Gemeinsame Geheimnisse	131
7.8.3.4	Vereinbarung eines gemeinsamen Geheimnisses	131

Teil B: Die Fahrzeugtechnik und der Einfluss der Cybersecurity..... 135

8	Automotive E/E-Systeme	137
8.1	Das Fahrzeug als System	137
8.2	Elektronische Steuergeräte	139
8.2.1	Einleitende Informationen	139
8.2.2	Steuergeräte-Hardware	143
8.2.2.1	Blockschaltbild	143
8.2.2.2	Analog-Digital- und Digital-Analog-Converter (ADC und DAC)	143

8.2.2.3	Steuergeräte-Speicher	144
8.2.3	Steuergeräte-Software	146
8.3	On-Board-Kommunikation	148
8.4	Serielle Bussysteme	149
8.4.1	Einleitende Informationen	149
8.4.2	Controller Area Network (CAN)	151
8.4.3	Local Interconnect Network (LIN)	164
8.4.4	In-Vehicle Ethernet (ETH)	166
8.5	E/E-System-Architekturen	166
9	Client-Server-Kommunikation	171
9.1	Das ISO/OSI-Schichtenmodell	171
9.2	Diagnose-Kommunikation	171
9.2.1	Diagnosedienste	171
9.2.2	Negative Response Codes (NRC)	175
9.2.3	Physikalische und funktionale Adressierung	175
9.2.4	Diagnostic Trouble Codes (DTC)	177
9.3	Diagnoseprotokolle (OSI-Application-Layer)	179
9.3.1	Einleitende Informationen	179
9.3.2	OBd II (ISO 15031)	183
9.3.3	UDS (ISO 14229)	188
9.3.3.1	Einleitende Informationen	188
9.3.3.2	Sub-Function-Bytes	189
9.3.3.3	Data Identifier (DID)	190
9.3.3.4	Negative Response Codes (NRC)	191
9.3.3.5	ALFID	192
9.3.3.6	Application Layer Services	192
9.3.4	WWH-OBd (ISO 27145)	201
9.3.5	OBDonUDS und ZEVonUDS (SAE J1979-x)	202
9.4	DoCAN (ISO 15765)	203
9.5	DoIP (ISO 13400)	206
10	Systemschnittstellen (OSI-Layer 1)	215
10.1	Der Diagnose-Steckverbinder	215
10.2	Ladestecker für Elektrofahrzeuge und Plug-in-Hybride	218
10.3	Funkschnittstellen	220
11	Diagnose-Clients	223
11.1	Einleitende Informationen	223
11.2	UML, XML und ODX	226
11.3	Diagnose-Spezifikationen	229
11.4	Diagnose-Sequenzen	238
11.4.1	Einleitende Informationen	238
11.4.2	Java-Jobs	239
11.4.3	OTX (ISO 13209)	239
11.5	Diagnose-Laufzeitsysteme	243

11.6	Vehicle Communication Interfaces (VCIs)	244
11.6.1	Einleitende Informationen	244
11.6.2	CAN-Interfaces mit CAN-L2-API	246
11.6.3	Pass-Thru Devices mit SAE J2534 API	248
11.6.4	VCIs mit RP1210B API	250
11.6.5	VCIs mit D-PDU API	250
11.6.6	OBD-Dongles	253
11.6.7	OEM-spezifische VCIs	255
12	Das Fahrzeug im Produktlebenszyklus	259
12.1	Der Produktlebenszyklus in der Prozesskette des Fahrzeugherstellers	259
12.2	Produktentstehungsprozess	259
12.3	Fahrzeugproduktion	261
12.4	Aftersales	263
12.4.1	Gewährleistung und Garantie	263
12.4.2	Fahrzeugherstellerabhängige Marktbeteiligte im Aftersales	263
12.4.2.1	Markengebundene Werkstätten	263
12.4.2.2	Markenspezifische Werkstattausrüstung	264
12.4.3	Fahrzeugherstellerunabhängige Marktbeteiligte im Aftersales	264
12.4.3.1	Einleitende Informationen	264
12.4.3.2	Freie Werkstätten	265
12.4.3.3	OEM-unabhängige Werkstattausrüster	265
12.4.3.4	Sachverständige und Prüforganisationen	266
12.4.3.5	Drittanbieter im Aftersales	266
12.4.4	Vorbereitung des OEM für das Aftersales	266
12.4.5	Das Änderungsmanagement des OEM im Aftersales	267
12.4.5.1	Änderungsmanagement vor EOP	268
12.4.5.2	Änderungsmanagement nach EOP	268
12.4.6	Umgang mit Altfahrzeugen	268
12.5	Einfluss der EU-Verordnung 2018/858 auf den Produktlebenszyklus	269
12.5.1	Typprüfung und Typgenehmigung	269
12.5.2	Delegierten-Verordnung (EU) 2022/2236	270
12.5.3	Rechte unabhängiger Marktbeteiligter	271
12.5.4	Cybersecurity im Produktlebenszyklus	272
13	Cybersecurity-Prozesse	275
13.1	Systembedrohungen	275
13.2	System- und Bedrohungsanalyse	276
13.3	UNECE R155 – CSMA und Typgenehmigung	279
13.3.1	Einführende Informationen	279
13.3.2	Übersicht der Bedrohungen	279
13.3.3	Minderungsmaßnahmen	281
13.4	ISO 21434 – Cybersecurity Engineering	281
13.5	UNECE R156 – Softwareaktualisierung im Aftersales	282
13.6	EU-Richtlinie 2022/2555 (NIS-2)	284
13.7	TISAX	284

13.8	Prozesse in der Werkstatt	285
13.8.1	Einführende Informationen	285
13.8.2	Datenmanagement in Werkstätten	286
13.8.2.1	Dienste im Workshop-Net	287
13.8.2.2	Netzwerkmanager	289
13.8.2.3	Senden und Nachfragen von Daten	291
13.8.2.4	Workshop-Net-API	292
13.8.2.5	Beispielablauf für eine Emissionsmessung	292
13.8.3	Cybersecurity in DMS und Workshop-Net	294
13.8.4	Zugang des Servicetesters zu einem Fahrzeug	295
13.8.5	Erweiterte Zugangsverfahren des Servicetesters	296
13.8.5.1	Markengebundene Werkstätten mit markengebundenen Testern	296
13.8.5.2	Freie Werkstätten und Prüforganisationen mit Mehrmarkengeräten	297
13.8.5.3	Erweiterung in verschiedene Autorisierungsebenen	298
13.8.5.4	Zugangsverfahren ohne Echtzeitzugang zum Herstellerportal	300
13.8.6	Sonstige Zugangsverfahren zu Herstellerportalen	300

Teil C: Konkrete Bedrohungen und Minderungsstrategien..... 303

14	Schwachstellen und Sicherheitslücken	305
14.1	Einleitende Informationen	305
14.2	Bekannte Schwachstellen (CVE und CWE)	306
14.3	Sicherheitslücken in vernetzten Fahrzeugen	307
15	Schützenswerte Informationen	309
15.1	Einleitende Informationen	309
15.2	Fahrzeugidentifikationsnummer (FIN)	309
15.2.1	Einleitende Informationen	309
15.2.2	Lesen der FIN mit UDS-Request 0x22 und DoCAN	313
15.2.3	Lesen der FIN mit UDS-Request 0x22 und DoIP	314
15.2.3.1	Einleitende Informationen	314
15.2.3.2	Analyse des UDS on IP Requests 0x22	316
15.3	Teilenummern und Komponentenschutz	319
15.4	Personenbezogene Daten	319
15.5	Steuergeräte-Software	320
15.6	Schaltpläne des E/E-Systems	320
15.7	Kommunikationsparameter	321
15.7.1	ODX, OTX und CBF	321
15.7.2	Negative Response Codes (NRC)	321
15.7.3	Seed und Key	322
15.8	Kilometerstand	323
15.8.1	Einleitende Informationen	323
15.8.2	Technische Daten	323
15.8.3	Bedrohungsanalyse und Schutzbedarf	326
15.8.4	Minderungsmaßnahmen	329

15.8.5	Ausblick.....	330
15.9	Zustand der Antriebsbatterie (SOH).....	331
15.9.1	Einleitende Informationen.....	331
15.9.2	Technische Daten.....	333
15.9.3	Methoden zur Beurteilung des Zustands der Antriebsbatterie.....	334
15.9.4	Bedrohungsanalyse und Schutzbedarf.....	337
15.9.5	Minderungsmaßnahmen.....	339
15.9.6	Ausblick.....	339
15.10	OBFCM-Daten.....	341
15.10.1	Einleitende Informationen.....	341
15.10.2	Technische Daten.....	342
15.10.3	Methoden zur Beurteilung der OBFCM-Daten.....	342
15.10.4	Bedrohungsanalyse und Schutzbedarf.....	344
15.10.5	Minderungsmaßnahmen.....	345
16	Schützenswerte Funktionen.....	347
16.1	Einleitende Informationen.....	347
16.2	On-Board-Kommunikation.....	348
16.2.1	Einleitende Informationen.....	348
16.2.2	Schwachstelle CAN-Bus.....	348
16.2.3	Schwachstelle In-Vehicle Ethernet.....	351
16.3	Diagnose-Kommunikation.....	353
16.3.1	Einleitende Informationen.....	353
16.3.2	Diagnoseschnittstelle und Sicherheits-Gateways.....	354
16.3.2.1	US Congress, NHTSA und SAE J3138.....	354
16.3.2.2	EU-Verordnung 2018/858 und der Europäische Gerichtshof (EuGH).....	357
16.3.3	Angriffsvektor Diagnosedienste (OBD/UDS).....	358
16.4	Kommunikation von E-Fahrzeugen mit Ladeinfrastruktur.....	359
16.5	V2X-Kommunikation über Funkschnittstellen.....	363
16.6	Automatisiertes Fahren.....	365
16.6.1	Fahrzeug-Automatisierung.....	365
16.6.2	Fahrerassistenzsysteme (ADAS).....	367
16.7	Abgasreinigung von Dieselmotoren.....	368
16.8	Reifendrucküberwachung.....	371
16.9	eCall (Emergency Call).....	371
16.10	Ferndiagnose und Ferndatenerfassung.....	372
16.11	Infotainmentsysteme.....	375
16.11.1	Einleitende Informationen.....	375
16.11.2	Navigation.....	375
16.11.3	Bluetooth-Verbindungen im Fahrzeug.....	375
16.11.4	WLAN-Hotspot-Verbindungen.....	377
16.12	Funkschlüssel und Keyless Entry & Go.....	378
16.13	Elektronische Wegfahrsperre.....	380
16.14	Funkschlüssel-Programmierung.....	381
16.15	Unfalldatenspeicher.....	383
16.16	Steuergeräte-Programmierung.....	384

16.16.1	Einleitende Informationen	384
16.16.2	Flashdatei und Flashware.....	384
16.16.3	Motorola S-Records	385
16.16.4	Flash-Prozesse	386
16.16.5	Bedrohungsanalyse und Angriffsvektoren	390
16.17	OTA-Updates	394
16.17.1	Einleitende Informationen	394
16.17.2	Manipulation des Update-Pakets	394
16.17.3	Kompromittierte OTA-Backend-Systeme	394
16.17.4	Man-in-the-Middle (MitM) während der Übertragung	394
16.17.5	Ausnutzung von Debug- oder Entwicklerzertifikaten	395
16.17.6	Missbrauch von Update-Triggern.....	395
16.17.7	Unzureichende Kontrolle über Update-Policy	395
16.17.8	Fehlende Protokollierung und Nachvollziehbarkeit	395
17	Anhang.....	397
17.1	Abkürzungsverzeichnis.....	397
17.2	Glossar	403
17.3	Literaturverzeichnis	406
17.3.1	Bücher	406
17.3.2	SAE Technical Papers	407
17.3.3	Vorlesungen	408
17.4	Übersicht ISO-Standards.....	409
17.5	Übersicht SAE Recommended Practices.....	411
	Stichwortverzeichnis	413