

Inhaltsverzeichnis

1	Einleitung	1
1.1	Motivation	1
1.2	Kapitelstruktur	2
	Literatur	4
2	Grundlagen der Informationssicherheit	5
2.1	Motivation	7
2.1.1	Informationssicherheit	8
2.1.2	Studien-Erkenntnisse	11
2.2	Sicherheit und Sicherheitsziele	15
2.2.1	Informationssicherheit – Charakteristik – Schutzziele	18
2.2.2	Fundamente der Informationssicherheit	22
2.2.3	Definitionen im Zusammenhang mit der Informationssicherheit	24
2.2.4	Social Engineering	25
2.2.4.1	Social Engineering – Beispiele	26
2.2.4.2	Social Engineering – Angriffsziele	29
2.2.5	Bug-Bounty-Programme – Honeypot	30
2.2.5.1	Bug-Bounty-Programm	31
2.2.5.2	Honeypot	31
2.3	Sicherheit der Verarbeitung	32
2.3.1	Technische Sicherungsmaßnahmen	33
2.3.2	Organisatorische Sicherungsmaßnahmen	33
2.3.3	Organisation und Compliance	34
2.3.4	Informationen sammeln	34
2.3.5	Self-Assessment	34
2.3.6	Teststrategien	35
2.3.7	Zeitenwende nach Stuxnet	37
2.4	NIS-Richtlinie	38

2.5	Zusammenfassung	40
	Literatur	41
3	Datenschutz (Privacy)	45
3.1	Motivation/Ursprung	46
3.1.1	Datenschutzgrundprinzipien: Konzepte	46
3.1.2	Datenschutz: Historie	47
3.1.3	Datenschutz: Charakteristik und Datenschutzziele	49
3.2	Basis der EU-DSGVO: Bundesdatenschutzgesetz n. F.	51
3.2.1	Bundesdatenschutzgesetz n. F.	51
3.2.2	EU-Datenschutz-Grundsatzverordnung	52
3.2.3	ePrivacy: Telekommunikation-Telemedien-Datenschutz-Gesetz	53
3.2.4	Personenbezogene Daten	54
3.2.5	Rechtmäßigkeit der Verarbeitung	56
3.3	Wichtige Artikel der EU-DSGVO	57
3.3.1	Grundsätze zur Verarbeitung personenbezogener Daten	58
3.3.2	Bedingungen für die Einwilligung	59
3.3.3	Sicherheit der Verarbeitung	60
3.3.4	Rechte der betroffenen Person	61
3.3.5	Datenschutz-Folgenabschätzung	62
3.3.6	Allgemeine Bedingungen für die Verhängung von Geldbußen	62
3.4	Privacy Engineering – Privacy-by-Design	63
3.4.1	Privacy Engineering	64
3.4.2	Sieben fundamentale Prinzipien: Privacy-by-Design (PbD)	66
3.4.3	Privacy-Strategien	71
3.5	Privacy-Enhancing-Technologies (PET)	73
3.6	Privacy-Risk-Modell (Datenschutz-Risikomodell)	76
3.6.1	Privacy-Risikoanalyse	76
3.6.2	Datenschutz-Bedrohungsmodellierung: LINDDUN	78
3.7	Datenschutz-Framework	81
3.8	Zusammenfassung	83
	Literatur	85
4	Funktionale Sicherheit (Safety)	89
4.1	Motivation	90
4.2	Ziele – Funktionale Sicherheit – Charakteristik	92
4.3	Schnittstelle Funktionale Sicherheit – Cybersecurity	97
4.3.1	Schnittstellen in der Automotive-Safety-Norm	98
4.3.2	Artverwandte Analyse-Methoden	100
4.3.3	SOTIF – Safety of the intended functionality	101
4.3.4	STPA – Systems Theoretic Process Analysis	102
4.3.5	Künstliche Intelligenz	103

4.4 Zusammenfassung	103
Literatur.	105
5 Informations-/Cybersecurity-Standards.	107
5.1 Security Development Lifecycle: Standards	108
5.1.1 Microsoft Security-Development-Lifecycle (SDL)	109
5.1.2 IEEE Cyber Security – Design Flaws	111
5.1.2.1 Die Top 10-Design-Mängel.	111
5.1.2.2 Gegenmaßnahmen zur Vermeidung der Top 10-Design-Mängel	112
5.1.3 Automotive SPICE®	114
5.2 Security-Standards	116
5.2.1 SAE International J3061™ ISO/SAE 21434	116
5.2.2 FIPS PUB 199/FIPS PUB 200/NIST SP 800-53	118
5.2.2.1 FIPS PUB 199 – Security Categorization	119
5.2.2.2 FIPS PUB 200 – Minimale Sicherheitsanforderungen	120
5.2.3 NIST SP 800-Reihe	120
5.2.4 ISA/IEC 62443 – IT-Sicherheit für Netze und Systeme	122
5.2.4.1 ISA/IEC 62443 – Ziele	122
5.2.4.2 ISA/IEC 62443 – Struktur der Normenreihe	124
5.2.4.3 ISA/IEC 62443 – Fundamentale Konzepte (Foundational Requirements)	125
5.2.5 27k-Familie – Informationssicherheit	130
5.2.5.1 ISO/IEC 27001 – Informationssicherheits- Management	131
5.2.5.2 ISO/IEC 27005 Security Risk Management	132
5.2.5.3 ISO/IEC 27701 – Datenschutz- Managementsystem.	132
5.2.6 TISAX – Automotive ISMS	132
5.2.7 UNECE/NHTSA – Automotive Regulierungen	133
5.2.8 IEC 15480 – Common Criteria	136
5.2.9 RTCA DO 326-A – Sicherheit in der Luftfahrt	139
5.2.10 EU Cybersecurity Act	140
5.3 Zusammenfassung	141
5.3.1 Secure Software Engineering	142
5.3.2 Herausforderungen und Maßnahmen	142
Literatur.	143
6 Hacking	147
6.1 Denkweise (Mindset)	148
6.2 Hacking-Beispiele	152
6.2.1 Google-Hacking	152

6.2.2	Passwort-Hacking	152
6.3	Hacking-Beispiel Automotive	153
6.3.1	Konnektivität macht es möglich.	155
6.3.2	Beispiel: Roll-Jam-Technique (Replay-Attacke).....	157
6.3.3	Beispiel: (Key-) Relay-Station-Attacke	158
6.4	Cyber-Kill-Chain	159
6.5	Zusammenfassung	161
	Literatur	162
7	Risiko-Assessment	165
7.1	Übersicht	166
7.1.1	Prinzipien	167
7.1.2	Rahmenwerk	168
7.1.3	Prozess	169
7.1.4	Risikokriterien	170
7.2	Automotive TARA nach ISO/SAE 21434	172
7.2.1	Identifikation der zu schützenden Werte	172
7.2.2	Identifikation von Bedrohungsszenarien	174
7.2.3	Bestimmung der Auswirkungsschwere	175
7.2.4	Analyse der Angriffspfade	176
7.2.5	Bestimmung der Angriffsmachbarkeit	176
7.2.6	Bewertung des Risikos	178
7.2.7	Risikobehandlungsentscheidung	179
7.3	Sicherheitsrisikobewertung nach ISA/IEC 62443	179
7.4	Risikobewertung nach ISO/IEC 27005	181
7.5	Risikobewertung nach NIST SP 800-30	182
7.6	Risikobewertung nach HEAVENS	185
7.6.1	Bedrohungsanalyse	187
7.6.2	Risikobewertung	188
7.6.3	Sicherheitsanforderungen	189
7.7	Bedrohungsmodellierung: STRIDE	189
7.7.1	STRIDE-per-Element	191
7.7.2	STRIDE-per-Interaktion	191
7.8	Zusammenfassung	192
	Literatur	193
8	IT-Service-Management	195
8.1	Motivation (Einbettung)	198
8.2	ITIL und COBIT	199
8.2.1	ITIL – IT Infrastructure Library	200
8.2.2	COBIT – Control Objectives for Information and Related Technology	201

8.3	27k – Informationssicherheits-Managementsystem	201
8.4	IT-Grundschutz-Kompendium	202
8.4.1	BSI-Standards zur Umsetzung	204
8.4.2	BSI-Risioanalyse	208
8.5	Der IT-Sicherheits-Beauftragte	209
	Literatur	210
9	Anhang: Kontrollfamilien	213
9.1	Kontrollfamilien für Security und Privacy	214
	Literatur	221
	Glossar	223
	Stichwortverzeichnis	233